OSTWALD'S KLASSIKER
DER EXAKTEN WISSENSCHAFTEN.
Nr. 122.

Sechs Beweise

des

Fundamentaltheorems über quadratische Reste

von

Carl Friedrich Gauss.

WILHELM ENGELMANN IN LEIPZIG.

Ankündigung.

Der grossartige Aufschwung, welchen die Naturwissenschaften in unserer Zeit erfahren haben, ist, wie allgemein anerkannt wird, wohl zum kleinsten Maasse durch die Ausbildung und Verbreitung der Unterrichtsmittel, der Experimentalvorlesungen, Laboratorien u. s. w., bedingt. Während aber durch die vorhandenen Einrichtungen zwar die Kenntniss des gegenwärtigen Inhaltes der Wissenschaft auf das erfolgreichste vermittelt wird, haben hochstehende und weitblickende Männer wiederholt auf einen Mangel hinweisen müssen, welcher der gegenwärtigen wissenschaftlichen Ausbildung jüngerer Kräfte nur zu oft anhaftet. Es ist dies das Fehlen des historischen Sinnes und der Mangel an Kenntniss jener grossen Arbeiten, auf welchen das Gebäude der Wissenschaft ruht.

Diesem Mangel soll durch die Herausgabe der Klassiker der exakten Wissenschaften abgeholfen werden. In handlicher Form und zu billigem Preise sollen die grundlegenden Abhandlungen der gesammten exakten Wissenschaften den Kreisen der Lehrenden und Lernenden zugänglich gemacht werden. Es soll dadurch ein Unterrichtsmittel beschafft werden, welches das Eindringen in die Wissenschaft gleichzeitig belebt und vertieft. Dasselbe ist aber auch ein Forschungsmittel von grosser Bedeutung. Denn in jenen grundlegenden Schriften ruhten nicht nur die Keime, welche inzwischen sich entwickelt und Früchte getragen haben, sondern es ruhen in ihnen noch zahllose andere Keime, die noch der Entwicklung harren, und dem in der Wissenschaft Arbeitenden und Forschenden bilden jene Schriften eine unerschöpfliche Fundgrube von Anregungen und fördernden Gedanken.

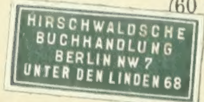
Die Klassiker der exakten Wissenschaften sollen ihrem Namen gemäss die rationellen Naturwissenschaften, von der Mathematik bis zur Physiologie umfassen und werden Abhandlungen aus den Gebieten der Mathematik, Astronomie, Physik, Chemie (einschliesslich Krystallkunde) und Physiologie enthalten.

Die allgemeine Redaktion führt von jetzt ab Professor Dr. Arthur von Oettingen (Leipzig); die einzelnen Ausgaben werden durch hervorragende Vertreter der betreffenden Wissenschaften besorgt werden. Die Leitung der einzelnen Abtheilungen übernahmen: für Astronomie Prof. Dr. Bruns (Leipzig), für Mathematik Prof. Dr. Wangerin (Halle), für Krystallkunde Prof. Dr. Groth (München), für Pflanzenphysiologie Prof. Dr. W. Pfeffer (Leipzig), für Chemie Prof. Dr. W. Ostwald (Leipzig).

Erschienen sind bis jetzt aus dem Gebiete der

Mathematik:

Nr. 2. **C. F. Gauss**, Allg. Lehrsätze in Beziehung auf die im verkehrten Verhältnisse des Quadrats der Entfernung wirkenden Anziehungs- und Abstossungs-Kräfte. (1840.) Herausgeg. v. A. Wangerin. (60 S.) *M* —.80.



5. **C. F. Gauss,** Flächentheorie. (1827.) Deutsch herausg. v. A. Wangerin. Zweite revidirte Auflage. (64 S.) ℳ —.80.

14. **C. F. Gauss,** Die 4 Beweise der Zerlegung ganzer algebr. Functionen etc. (1799—1849.) Herausg. v. E. Netto. Mit 1 Taf. (81 S.) ℳ 1.50.

17. **A. Bravais,** Abhandlungen über symmetr. Polyeder. (1849.) Übers. und in Gemeinschaft mit P. Groth herausg. von C. u. E. Blasius. Mit 1 Taf. (50 S.) ℳ 1.—.

19. Üb. d. Anziehung homogener Ellipsoide. Abhandlungen von **Laplace** (1782), **Ivory** (1809), **Gauss** (1813), **Chasles** (1838) und **Dirichlet** (1839). Herausg. von A. Wangerin. (118 S.) ℳ 2.—.

16. Abhandlungen über Variations-Rechnung. I. Theil: Abhandlungen von **Joh. Bernoulli** (1696), **Jac. Bernoulli** (1697) und **Leonhard Euler** (1744). Herausgegeben von P. Stäckel. Mit 19 Textfiguren. (144 S.) ℳ 2.—.

17. —— —— II. Theil: Abhandlungen von **Lagrange** (1762, 1770), **Legendre** (1786) und **Jacobi** (1837). Herausgegeben von P. Stäckel. Mit 12 Textfiguren. (110 S.) ℳ 1.60.

54. **J. H. Lambert,** Anmerkungen und Zusätze zur Entwerfung der Land- und Himmelscharten. (1772.) Herausgeg. von A. Wangerin. Mit 21 Textfiguren. (96 S.) ℳ 1.60.

55. **Lagrange** u. **Gauss,** Abhandlungen über Kartenprojection. (1779 und 1822.) Herausgeg. von A. Wangerin. Mit 2 Textfiguren. (102 S.) ℳ 1.60.

60. **Jacob Steiner,** Die geometr. Constructionen, ausgeführt mittelst der geraden Linie und eines festen Kreises, als Lehrgegenstand auf höheren Unterrichts-Anstalten und zur praktischen Benutzung. (1833.) Herausgegeben von A. J. v. Oettingen. Mit 25 Textfiguren. (85 S.) ℳ 1.20.

64. **C. G. J. Jacobi,** Über die vierfach periodischen Functionen zweier Variabeln, auf die sich die Theorie der Abel'schen Transcendenten stützt. (1834.) Herausgegeben von H. Weber. Aus dem Lateinischen übersetzt von A. Witting. (40 S.) ℳ —.70.

65. **Georg Rosenhain,** Abhandlung über die Functionen zweier Variabler mit vier Perioden, welche die Inversen sind der ultraelliptischen Integrale erster Klasse. (1851.) Herausgegeben von H. Weber. Aus dem Französischen übersetzt von A. Witting. (94 S.) ℳ 1.50.

67. **A. Göpel,** Entwurf einer Theorie der Abel'schen Transcendenten erster Ordnung. (1847.) Herausgegeben von H. Weber. Aus dem Lateinischen übersetzt von A. Witting. (60 S.) ℳ 1.—.

71. **N. H. Abel,** Untersuchungen über die Reihe:

$$1+\frac{m}{1}x+\frac{(m\cdot m-1)}{1\cdot 2}\cdot x^2+\frac{m\cdot(m-1)\cdot(m-2)}{1\cdot 2\cdot 3}\cdot x^3+\cdots$$

(1826.) Herausgegeben von A. Wangerin. (46 S.) ℳ 1.—.

73. **Leonhard Euler,** Zwei Abhandlungen über sphärische Trigonometrie. Grundzüge der sphärischen Trigonometrie und allgemeine sphärische Trigonometrie. (1753 u. 1779.) Aus dem Französischen und Lateinischen übersetzt und herausgegeben von E. Hammer. Mit 6 Figuren im Text. (65 S.) ℳ 1.—.

77. **C. G. J. Jacobi,** Über die Bildung und die Eigenschaften der Determinanten. (De formatione et proprietatibus Determinantium.) (1841.) Herausgegeben von P. Stäckel. (73 S.) ℳ 1.20.

78. **J. C. G. Jacobi,** Über die Functionaldeterminanten. (De determinantibus functionalibus.) (1841.) Herausgegeben von P. Stäckel. (72 S.) ℳ 1.20.

Nr. 82. **Jacob Steiner,** Systematische Entwicklung der Abhängigkeit geometrischer Gestalten von einander, mit Berücksichtigung der Arbeiten alter und neuer Geometer über Porismen, Projections-Methoden, Geometrie der Lage, Transversalen, Dualität und Reciprocität etc. (1832.) I. Theil. Herausgegeben von A. J. v. Oettingen. Mit 2 Tafeln und 14 Fig. im Text. (126 S.) ℳ 2.—.

» 83. —— —— II. Theil. Herausgegeben von A. J. v. Oettingen. Mit 2 Tafeln und 2 Figuren im Text. (162 S.) ℳ 2.40.

» 90. **A. Bravais,** Abhandlung über die Systeme von regelmässig auf einer Ebene oder im Raum vertheilten Punkten. (1848.) Übers. u. herausgegeben von C. u. E. Blasius. Mit 2 Tafeln. (142 S.) ℳ 2.—.

» 91. **G. Lejeune Dirichlet,** Untersuchungen über verschiedene Anwendungen der Infinitesimalanalysis auf die Zahlentheorie. (1839 bis 1840.) Deutsch herausgegeben von R. Haussner. (128 S.) ℳ 2.—.

» 93. **Leonhard Euler,** Drei Abhandlungen über Kartenprojection. (1777). Mit 9 Textfig. Herausg. von A. Wangerin. (78 S.) ℳ. 1.20.

» 103. **Joseph Louis Lagrange's** Zusätze zu Euler's Elementen der Algebra. Unbestimmte Analysis. Aus dem Französischen übersetzt von A. J. von Oettingen, herausg. von H. Weber. (171 S.) ℳ 2.60.

» 107. **Jakob Bernoulli,** Wahrscheinlichkeitsrechnung (Ars conjectandi). (1713.) I. u. II. Theil. Übersetzt und herausgegeben von R. Haussner. Mit 1 Figur im Text. (162 S.) ℳ 2.50.

» 108. —— —— III. u. IV. Theil mit dem Anhange: Brief an einen Freund über das Ballspiel (Jeu de Paume). Übersetzt und herausgegeben von R. Haussner. Mit 3 Fig. (172 S.) ℳ 2.70.

» 111. **N. H. Abel,** Abhandlung über eine besondere Klasse algebraisch auflösbarer Gleichungen. Herausgegeben von Alfred Loewy. (50 S.) ℳ —.90.

» 112. **Augustin-Louis Cauchy,** Abhandlung über bestimmte Integrale zwischen imaginären Grenzen (1825). Herausgegeben von P. Stäckel. (80 S.) ℳ 1.25.

» 113. **Lagrange** (1772) und **Cauchy** (1819), Zwei Abhandlungen zur Theorie der partiellen Differentialgleichungen erster Ordnung. Aus dem Französischen übersetzt und herausgegeben von Dr. Gerhard Kowalewski. (54 S.) ℳ 1.—.

» 116. **Lejeune Dirichlet,** Die Darstellung ganz willkürlicher Functionen durch Sinus- und Cosinusreihen (1837) und **Philipp Ludwig Seidel,** Note über eine Eigenschaft der Reihen, welche discontinuirliche Functionen darstellen (1847). Herausgegeben von Heinrich Siebmann. (58 S.) ℳ 1.—.

» 117. **Gaspard Monge,** Darstellende Geometrie (1798). Übersetzt und herausgegeben von Robert Haussner. Mit zahlreichen Figuren in dem Texte und in den Anmerkungen. (217 S.) ℳ 4.—.

» 122. **Carl Friedrich Gauss,** Sechs Beweise des Fundamentaltheorems über quadratische Reste. Herausgegeben von Eugen Netto. (111 S.) ℳ 1.80.

Sechs Beweise

des

Fundamentaltheorems über quadratische Reste

von

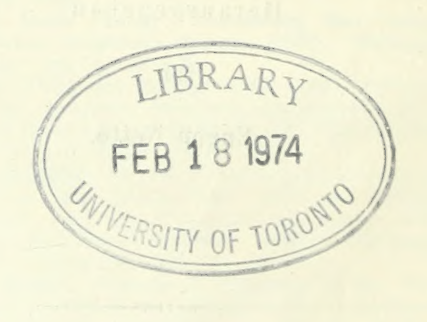
Carl Friedrich Gauss.

Herausgegeben

von

Eugen Netto.

Leipzig
Verlag von Wilhelm Engelmann
1901.


LIBRARY
FEB 18 1974
UNIVERSITY OF TORONTO



Erster Beweis des Fundamentaltheorems über quadratische Reste.[1])

Disquisitiones arithmeticae.

1801 Lipsiae; Fleischer jun.

(Werke, Bd. I; p. 73—111.)

Quadratische Reste und Nichtreste.

§ 94. Lehrsatz. Für irgend eine Zahl m als Modul können unter den Zahlen $0, 1, 2, 3, \ldots m-1$ bei geradem m nicht mehr als $\frac{1}{2}m+1$, bei ungeradem m nicht mehr als $\frac{1}{2}m+\frac{1}{2}$ einem Quadrate congruent sein.

Beweis. Da die Quadrate congruenter Zahlen einander congruent sind, so wird jede Zahl, die irgend einem Quadrate congruent ist, auch einem Quadrate congruent sein, dessen Wurzel $< m$ wird. Es reicht daher aus, die kleinsten Reste der Quadrate $0, 1, 4, 9, \ldots (m-1)^2$ zu betrachten. Nun sieht man leicht, dass $(m-1)^2 \equiv 1^2$, $(m-2)^2 \equiv 2^2$, $(m-3)^2 \equiv 3^2$ sei, u. s. f. Folglich werden bei geradem m die kleinsten Reste der Quadrate $(\frac{1}{2}m-1)^2$ und $(\frac{1}{2}m+1)^2$, $(\frac{1}{2}m-2)^2$ und $(\frac{1}{2}m+2)^2$ u. s. f. dieselben sein; wenn hingegen m ungerade ist, werden die Quadrate $(\frac{1}{2}m-\frac{1}{2})^2$ und $(\frac{1}{2}m+\frac{1}{2})^2$, $(\frac{1}{2}m-\frac{3}{2})^2$ und $(\frac{1}{2}m+\frac{3}{2})^2$, u. s. w. einander congruent. Daraus erhellt, dass bei geradem m nur solche Zahlen einem Quadrate congruent werden können, welche einem der Quadrate $0, 1, 4, 9, \ldots (\frac{1}{2}m)^2$ congruent sind; dass dagegen bei ungeradem m jede Zahl, die einem Quadrate congruent wird, nothwendig einem aus der Reihe $0, 1, 4, 9, \ldots (\frac{1}{2}m-\frac{1}{2})^2$ congruent sein muss. Es giebt also im ersten Falle höchstens $\frac{1}{2}m+1$ verschiedene kleinste Reste, im zweiten $\frac{1}{2}m+\frac{1}{2}$. W. z. b. w.

Beispiel. Für den Modul 13 findet man als kleinste Reste der Quadrate von $0, 1, 2, 3, \ldots 6$ die Zahlen 0, 1, 4, 9, 3, 12, 10; die weiteren Reste wiederholen sich in umgekehrter Folge 10, 12, 3 u. s. w. Jede Zahl, die keinem dieser Reste und daher einer der Zahlen 2, 5, 6, 7, 8, 11 congruent ist, kann keinem Quadrate congruent sein.

Für den Modul 15 findet man die Reste 0, 1, 4, 9, 1, 10, 6, 4, welche sich weiter in umgekehrter Ordnung wiederholen. Hier ist also die Zahl der Reste, welche einem Quadrate congruent werden können, noch kleiner als $\frac{1}{2}m + \frac{1}{2}$; es sind nämlich die Reste 0, 1, 4, 6, 9, 10. Die Zahlen 2, 3, 5, 7, 8, 11, 12, 13, 14 und die, einer von ihnen congruenten können mod. 15 keinem Quadrate congruent werden.

§ 95. Hieraus entnimmt man, dass für jeden Modul alle Zahlen in zwei Classen verteilt werden können, deren eine die Zahlen enthält, welche einem Quadrate congruent werden können, und die andere diejenigen Zahlen, die es nicht werden können. Jene wollen wir quadratische Reste der als Modul angenommenen Zahl nennen, diese hingegen quadratische Nichtreste derselben, oder auch, falls keine Zweideutigkeit daraus entspringen kann, kurz Reste und Nichtreste. Es reicht übrigens offenbar aus, alle Zahlen 0, 1, 2, ... $m - 1$ in diese Classen zu vertheilen, denn congruente Zahlen gehören in dieselbe Classe.

Bei diesen Untersuchungen gehen wir von den Primzahlen aus; dies ist festzuhalten, auch wenn es nicht ausdrücklich erwähnt wird. Die Primzahl 2 jedoch soll ausgeschlossen, und es sollen nur ungerade Primzahlen betrachtet werden.

Primzahl-Moduln.

§ 96. Ist eine Primzahl p Modul, so wird die Hälfte der Zahlen 1, 2, 3, ... $p - 1$ zu quadratischen Resten, die übrigen werden zu quadratischen Nichtresten, d. h. es giebt $\frac{1}{2}(p - 1)$ Reste und eben so viele Nichtreste.

Man kann nämlich leicht beweisen, dass alle Quadrate 1, 4, 9, . . . $\frac{1}{4}(p - 1)^2$ incongruent sind. Wäre etwa für die ungleichen Zahlen r, r', die nicht grösser als $\frac{1}{2}(p - 1)$ sind, bei $r > r'$ gleichwohl $r^2 \equiv r'^2$ (mod. p), so müsste $(r - r')$ $(r + r')$ positiv und durch p theilbar sein. Allein jeder der Factoren $r - r'$ und $r + r'$ ist kleiner als p; deshalb kann unsere Annahme nicht aufrecht erhalten werden. Es giebt also unter den Zahlen 1, 2, 3, . . . $p - 1$ genau $\frac{1}{2}(p - 1)$ quadratische Reste; und nicht mehr, weil nach Hinzunahme der Null $\frac{1}{2}(p + 1)$ entstehen, und dies die obere Grenze für die Anzahl der Reste ist. Folglich werden die übrigen Zahlen Nichtreste, und ihre Menge ist $= \frac{1}{2}(p - 1)$.

Da die Null stets Rest ist, so wollen wir sie und die durch den Modul theilbaren Zahlen von unseren Untersuchungen ausschliessen; denn dieser Fall, der an und für sich klar ist, würde nur den kurzen Ausdruck der Lehrsätze stören. Aus demselben Grunde haben wir auch den Modul 2 ausgeschlossen.

Zusammengesetzte Zahlen als Reste bei Primzahl-Moduln.

§ 98. Lehrsatz. Das Product aus zwei quadratischen Resten der Primzahl p ist ein Rest; das Product aus einem Reste und einem Nichtreste ist ein Nichtrest; endlich das Product aus zwei Nichtresten ein Rest.

Beweis. I. Sind A, B die Reste der Quadrate a^2, b^2, d. h. $A \equiv a^2$, $B \equiv b^2$, dann wird das Product AB dem Quadrate der Zahl ab congruent d. h. ein Rest sein.

II. Wenn A ein Rest und zwar $\equiv a^2$, B dagegen ein Nichtrest ist, dann wird AB ein Nichtrest. Wäre nämlich $AB \equiv k^2$, so könnten wir den Werth des Ausdruckes

$$k : a \,(\text{mod.}\, p) \equiv b$$

setzen; folglich würde $a^2 B \equiv a^2 b^2$, und daher $B \equiv b^2$, d. h. B gegen die Annahme ein Rest sein.

III. Seien A, B Nichtreste. Wir multipliciren alle Reste, die unter $1, 2, 3, \ldots p-1$ vorkommen, mit A; dadurch entstehen $\frac{1}{2}(p-1)$ unter einander incongruente Nichtreste nach II; keinem derselben kann das Product AB congruent sein; wäre es daher Nichtrest, so gäbe es $\frac{1}{2}(p+1)$ incongruente Nichtreste, gegen § 96. Daher ist das Product u. s. w. — W. z. b. w.

Noch leichter folgen diese Theoreme aus den Lehren der Index-Theorie. Da nämlich die Indices von Resten stets gerade sind, die von Nichtresten dagegen ungerade, so wird der Index des Productes zweier Reste oder zweier Nichtreste gerade und also das Product selbst ein Rest. Hingegen wird der Index eines Productes aus Rest und Nichtrest ungerade und also das Product selbst ein Nichtrest.

Beide Beweismethoden lassen sich auch für folgende Theoreme verwenden: Der Werth des Ausdruckes $\frac{a}{b}(\text{mod.}\, p)$ wird ein Rest sein, wenn die Zahlen a und b zugleich

Reste oder zugleich Nichtreste sind; dagegen wird er ein Nichtrest, wenn von den Zahlen a, b die eine Rest, die andere Nichtrest ist.

§ 99. Allgemein ist ein Product aus beliebig vielen Factoren ein Rest sowohl dann, wenn alle einzelnen Factoren Reste sind, als auch, wenn die Anzahl der unter die Factoren eingehenden Nichtreste gerade ist; wenn aber die Anzahl der eingehenden Nichtreste ungerade ist, dann wird das Product ein Nichtrest. Man kann daher leicht entscheiden, ob eine zusammengesetzte Zahl Rest ist oder nicht, sobald dies von ihren einzelnen Factoren bekannt ist.

Zusammengesetzte Zahlen als Moduln.

§ 100. Bevor wir zu schwierigeren Dingen übergehen, muss Einiges über Moduln beigebracht werden, welche keine Primzahlen sind.

Wird als Modul eine beliebige Potenz p^n der Primzahl p genommen, wobei p von 2 verschieden sein soll, dann wird die eine Hälfte aller durch p nicht theilbaren Zahlen, welche kleiner als der Modul sind, Reste und die andere Hälfte Nichtreste, d. h. die Anzahl der Individuen jeder Sorte ist $= \frac{1}{2}(p-1)p^{n-1}$.

r wird nämlich, wenn es ein Rest ist, irgend einem Quadrate congruent, dessen Wurzel die Hälfte des Moduls nicht übertrifft (§ 94). Nun sieht man leicht, dass es $\frac{1}{2}(p-1)p^{n-1}$ Zahlen giebt, die durch p nicht theilbar und kleiner als die Hälfte des Moduls sind. Es braucht also nur bewiesen zu werden, dass die Quadrate aller dieser Zahlen incongruent seien, d. h. dass sie verschiedene quadratische Reste liefern. Sind nun a, b zwei durch p nicht theilbare Zahlen, die kleiner sind als die Hälfte des Moduls, und würden ihre Quadrate einander congruent, so wäre $a^2 - b^2$ oder $(a-b)(a+b)$ durch p^n theilbar (wobei, was angeht, $a > b$ gesetzt werden mag). Jene Theilbarkeit kann aber nicht stattfinden, wenn nicht entweder eine der beiden Zahlen $a-b$, $a+b$ durch p^n theilbar wird, was unmöglich ist, da jede $< p^n$ bleibt; oder wenn die eine durch p^m, die andere durch p^{n-m}, d. h. jede durch p theilbar wird. Aber auch dies ist unmöglich. Denn offenbar würden auch die Summe und die Differenz $2a$ und $2b$ durch p theilbar werden, und also gegen die Voraussetzung auch a und b. — Hieraus folgt endlich, dass es unter den

durch p nicht theilbaren Zahlen, die kleiner als der Modul sind, $\frac{1}{2}(p-1)p^{n-1}$ Reste giebt, und dass die anderen, deren Anzahl die gleiche ist, quadratische Nichtreste sind. — W. z. b. w.

§ 101. Jede durch p nicht theilbare Zahl, welche Rest von p ist, wird auch Rest von p^n; ist sie aber Nichtrest von p, so wird sie auch Nichtrest von p^n.

Der zweite Teil dieser Behauptung ist an sich klar. Wäre daher der erste falsch, so würde es unter den Zahlen, die kleiner als p^n und durch p nicht theilbar sind, mehr Reste für p geben als für p^n, d. h. mehr als $\frac{1}{2}p^{n-1}(p-1)$. Ohne Mühe erkennt man aber, dass unter den angegebenen Zahlen genau $\frac{1}{2}p^{n-1}(p-1)$ Reste von p vorkommen.

Ebenso leicht ist es, ein Quadrat selbst zu finden, welches mod. p^n einem gegebenen Reste congruent ist, wenn man ein Quadrat kennt, welches diesem Reste mod. p congruent ist.

Kennt man nämlich a^2 als ein Quadrat, welches dem vorgelegten Reste A nach dem Modul p^μ congruent ist, dann kann man hieraus ein Quadrat herleiten, welches $\equiv A \pmod{p^\nu}$ wird, wobei $\nu > \mu$ und $=$ oder $< 2\mu$ anzunehmen ist. Wir setzen die Wurzel des gesuchten Quadrates in die Form $\pm a + xp^\mu$, deren Berechtigung leicht erkannt wird; dann muss $a^2 \pm 2axp^\mu + x^2p^{2\mu} \equiv A \pmod{p^\nu}$ oder wegen $2\mu \geqq \nu$ auch $A - a^2 \equiv \pm 2axp^\mu \pmod{p^\nu}$ sein. Ist $A - a^2 = p^\mu d$, dann wird x der Werth des Ausdruckes $\pm \frac{d}{2a} \pmod{p^{\nu-\mu}}$ oder des ihm äquivalenten $\pm \frac{A - a^2}{2ap^\mu} \pmod{p^\nu}$.

Ist also ein Quadrat gegeben $\equiv A \pmod{p}$, so kann daraus ein Quadrat $\equiv A \pmod{p^2}$ hergeleitet werden; von da kann man zum Modul p^4, von da zu p^8, . . . aufsteigen.

Beispiel. Ist der Rest 6 vorgelegt, welcher $\equiv 1^2 \pmod{5}$ ist, so findet man, dass er $\equiv 9^2 \pmod{25}$, $\equiv 16^2 \pmod{125}$ u. s. w. wird.

§ 102. Gehen wir nun zu den durch p theilbaren Zahlen über, so werden offenbar ihre Quadrate durch p^2 theilbar sein; folglich werden alle, zwar durch p aber nicht durch p^2 theilbaren Zahlen Nichtreste für p^n sein. Wird allgemein p^kA vorgelegt, wo A durch p nicht theilbar ist, dann sind folgende Fälle zu unterscheiden:

1) Ist $k \geqq n$, dann wird $p^k A \equiv 0$ (mod. p^n) und also Rest.

2) Ist $k < n$ und ungerade, dann wird $p^k A$ Nichtrest.

Wäre nämlich $p^k A = p^{2\varkappa+1} A \equiv s^2$ (mod. p^n), so wäre s^2 durch $p^{2\varkappa+1}$ theilbar, was nur möglich ist, wenn s durch $p^{\varkappa+1}$ theilbar wird. Dann wäre aber s^2 auch durch $p^{2\varkappa+2}$ theilbar, und also auch (weil $2\varkappa+2$ sicher nicht grösser als n ist) $p^k A$, d. h. $p^{2\varkappa+1} A$, oder gegen die Voraussetzung A durch p.

3) Ist $k < n$ und gerade, dann wird $p^k A$ Rest oder Nichtrest von p^2 sein, je nachdem A Rest bezw. Nichtrest von p ist. Wenn nämlich A Rest von p ist, so wird es auch Rest von p^{n-k}; und setzen wir $A \equiv a^2$ (mod. p^{n-k}), dann wird $Ap^k \equiv a^2 p^k$ (mod. p^n), und $a^2 p^k$ ist ein Quadrat. Ist aber A Nichtrest von p, dann kann nicht $p^k A$ Rest von p^n sein. Setzen wir nämlich $p^k A \equiv a^2$ (mod. p^n), so wird nothwendigerweise a^2 durch p^k theilbar. Der Quotient wird ein Quadrat, dem A modulo p^{n-k} und also auch modulo p congruent ist, d. h. A wird gegen die Voraussetzung ein Rest von p.

§ 103. Ueber den bisher ausgeschlossenen Fall $p = 2$ ist noch Einiges zu sagen. Für den Modul 2 wird jede Zahl Rest, und keine Nichtrest. Für den Modul 4 werden alle ungeraden Zahlen von der Form $4k+1$ Reste, alle jedoch von der Form $4k+3$ Nichtreste. Wird endlich 8 oder eine höhere Potenz von 2 zum Modul genommen, so werden alle ungeraden Zahlen von der Form $8k+1$ Reste, die übrigen jedoch, d. h. die von einer der Formen $8k+3$, $8k+5$, $8k+7$ werden Nichtreste. Der letzte Theil dieses Satzes folgt daraus, dass das Quadrat einer jeden ungeraden Zahl, gleichgültig, ob sie die Form $4k+1$ oder $4k-1$ hat, von der Form $8k+1$ wird. Den ersten Theil beweisen wir so:

1) Wenn die Summe oder die Differenz zweier Zahlen durch 2^{n-1} theilbar ist, dann werden die Quadrate dieser Zahlen einander modulo 2^n congruent. Denn ist die eine $= a$, so hat die andere die Form $2^{n-1}h \pm a$, und das Quadrat hiervon wird $\equiv a^2$ (mod. 2^n).

2) Jede ungerade Zahl, welche quadratischer Rest von 2^n ist, wird einem Quadrate congruent, dessen Wurzel ungerade und $< 2^{n-2}$ ist. Ist nämlich a^2 irgend ein Quadrat, welchem jene Zahl congruent ist, und hat man $a \equiv \pm \alpha$ (mod. 2^{n-1}), so dass α die Hälfte des Moduls nicht übertrifft, dann folgt $a^2 \equiv \alpha^2$. Daher wird die vorgelegte Zahl $\equiv \alpha^2$. Offenbar sind a und α ungerade und $\alpha < 2^{n-2}$.

3) Die Quadrate aller ungeraden Zahlen, welche kleiner sind als 2^{n-2}, sind modulo 2^n incongruent. Wären nämlich r und s zwei solche Zahlen, deren Quadrate modulo 2^n congruent werden, dann würde $(r-s)(r+s)$ durch 2^n theilbar (dabei sei $r > s$). Nun sieht man leicht, dass $r-s$ und $r+s$ nicht zugleich durch 4 theilbar sein können; wenn dagegen die eine der beiden Zahlen nur durch 2 theilbar ist, müsste die andere durch 2^{n-1} theilbar werden, damit das Product durch 2^n theilbar wäre. Jede der beiden Zahlen r, s ist aber kleiner als 2^{n-2}, also u. s. w.: w. z. b. w.

4) Werden diese Quadrate endlich auf ihre kleinsten positiven Reste reducirt, so giebt es 2^{n-3} verschiedene quadratische Reste, welche kleiner als der Modul sind*), und deren jeder von der Form $8n+1$ wird. Da nun genau 2^{n-3} Zahlen von der Form $8n+1$ existiren, die kleiner als der Modul sind, so gehören diese alle zu jenen Resten. W. z. b. w.

Um ein Quadrat zu finden, welches einer gegebenen Zahl von der Form $8k+1$ modulo 2^n congruent ist, kann man eine Methode anwenden, welche der aus § 101 ähnlich ist. — Von geraden Zahlen gilt das, was in § 102 allgemein aus einander gesetzt wurde.

§ 104. Ueber die Anzahl der verschiedenen (d. h. nach dem Modul incongruenten) Werthe, welche der Ausdruck $V \equiv \sqrt{A}$ (mod. p^n) zulässt, falls A quadratischer Rest von p^n ist, ergiebt sich aus dem Besprochenen leicht das Folgende. (p setzen wir wie oben als Primzahl voraus und schliessen der Kürze halber den Fall $n=1$ sogleich ein). I. Wenn A durch p nicht theilbar ist, hat V einen Werth, nämlich $V \equiv 1$ für $p=2$, $n=1$: zwei, wenn p ungerade ist, und ebenso für $p=2$, $n=2$, derart dass, wenn der eine $\equiv r$ ist, der andere $\equiv -r$ wird; vier für $p=2$, $n>2$, derart dass, wenn man den einen $\equiv r$ setzt, die übrigen $\equiv -r$, $2^{n-1}+r$, $2^{n-1}-r$ werden. — II. Wenn A durch p theilbar ist, aber nicht durch p^n, dann sei die höchste Potenz von p, welche in A aufgeht, $p^{2\mu}$ (offenbar muss der Exponent gerade sein), und weiter sei $A = ap^{2\mu}$. Dann müssen sicher alle Werthe von V durch p^μ theilbar sein, und die Quotienten der Division werden die Werthe des Ausdruckes $V' \equiv \sqrt{a}$ (mod. $p^{n-2\mu}$).

*) Die Anzahl der ungeraden Zahlen unterhalb 2^{n-2} ist nämlich 2^{n-3}.

Aus ihnen gehen alle verschiedenen Werthe von V hervor, indem man alle Werthe von V', die zwischen 0 und $p^{n-\mu}$ liegen, mit p^{μ} multiplicirt. Sie werden daher durch

$$rp^{\mu},\ rp^{\mu}+p^{n-\mu},\ rp^{\mu}+2p^{n-\mu}, \ldots rp^{\mu}+(p^{\mu}-1)p^{n-\mu}$$

gegeben, wenn r unbestimmt alle verschiedenen Werthe von V' bedeutet: jene Anzahl wird daher p^{μ}, $2p^{\mu}$ oder $4p^{\mu}$, je nachdem diese Anzahl gemäss I) gleich 1, 2 oder 4 wird. — III. Wenn A durch p^n theilbar ist, dann erkennt man leicht, dass für $n = 2m$ oder $= 2m - 1$, je nachdem n gerade oder ungerade ist, alle durch p^m theilbaren und nur diese Zahlen Werthe von V sind. All diese verschiedenen Werthe sind also 0, p^m, $2p^m, \ldots (p^{n-m}-1)p^m$, und ihre Anzahl ist p^{n-m}.

§ 105. Es bleibt nur noch der Fall übrig, dass der Modul m aus mehreren Primzahlen zusammengesetzt ist. Es sei $m = a.b.c. \ldots$, wobei $a, b, c, \ldots$ verschiedene Primzahlen oder Potenzen verschiedener Primzahlen bedeuten. Man erkennt sofort, dass, wenn n ein Rest von m ist, dann n gleichfalls ein Rest für die einzelnen Factoren $a, b, c, \ldots$ sein wird, und dass folglich n sicher ein Nichtrest für m wird, wenn es Nichtrest irgend einer der Zahlen $a, b, c, \ldots$ sein sollte. — Wenn umgekehrt aber n ein Rest für alle einzelnen Factoren $a, b, c, \ldots$ ist, dann wird es auch ein Rest für ihr Product m sein. Denn nehmen wir an, es sei $n \equiv A^2, B^2, C^2, \ldots$ für die Moduln a, bezw. $b, c, \ldots$, und bestimmt man dann eine Zahl N, welche den Zahlen $A, B, C, \ldots$ nach den Moduln a, bezw. $b, c, \ldots$ congruent ist, dann wird $n \equiv N^2$ nach allen einzelnen Moduln und folglich auch nach deren Product m. — Nun sieht man leicht ein, dass auf diese Weise aus der Combination jedes Werthes von A, d. h. jedes Ausdruckes $\sqrt{n}$ (mod. a) mit jedem Werthe von B, mit jedem Werthe von C u. s. w. ein Werth von N, d. h. vom Ausdrucke $\sqrt{n}$ (mod. m) entsteht; und ferner, dass aus verschiedenen Combinationen verschiedene N entstehen und aus sämmtlichen Combinationen sämmtliche N. Daher wird die Anzahl der verschiedenen Werthe von N dem Producte aus den Anzahlen der Werthe von $A, B, C, \ldots$ gleich; und diese haben wir im § 104 zu bestimmen gelehrt. — Ferner ist es klar, dass, wenn ein Werth von $\sqrt{n}$ (mod. m) oder von N bekannt ist, dieser zugleich ein Werth von $A, B, C, \ldots$ wird; aus diesen kann

man nach den obigen Darlegungen alle übrigen Werthe von $A, B, C, \ldots$ herleiten; und so folgt leicht, dass man aus einem Werthe von X alle anderen erhalten kann.

Beispiel. Modul sei 315; man fragt, ob 46 für ihn Rest oder Nichtrest ist. Die verschiedenen Primtheiler von 315 sind 3, 5, 7; und 46 ist Rest für jeden und also auch für 315. Weil ferner $46 \equiv 1$ und $\equiv 64$ (mod. 9); $\equiv 1$ und $\equiv 16$ (mod. 5); $\equiv 4$ und $\equiv 25$ (mod. 7), so sind die Wurzeln der Quadrate, denen 46 modulo 315 congruent ist, 19, 26, 44, 89, 226, 271, 289, 296.

Allgemeines Kriterium für Reste und Nichtreste von Primzahlen.

§ 106. Wir müssen jetzt nach sicheren Kennzeichen dafür forschen, ob eine gegebene Primzahl Rest oder Nichtrest einer gegebenen Primzahl sei. Bevor wir aber an diese Untersuchung gehen, wollen wir ein gewisses Merkmal hierfür darlegen, welches zwar in der Praxis wenig Nutzen gewährt, seiner Einfachheit und Allgemeinheit halber jedoch der Mittheilung werth erscheint.

Eine jede, durch die Primzahl $2m+1$ nicht theilbare Zahl A ist für diese Primzahl Rest oder Nichtrest, je nachdem $A^m \equiv +1$ oder $\equiv -1$ (mod. $2m+1$) ist.

Ist nämlich in irgend einem Index-Systeme für den Modul $2m+1$ der Index von A gleich a, so wird a gerade, wenn A Rest für $2m+1$ ist, ungerade hingegen, wenn A Nichtrest ist. Nun ist der Index von A^m gleich ma d. h. $\equiv 0$ oder $\equiv m$ (mod. $2m$), je nachdem a gerade oder ungerade ist. Demnach wird A^m im ersten Falle $\equiv +1$, im zweiten hingegen $\equiv -1$ (mod. $2m+1$).

Beispiel. 3 ist Rest für 13, weil $3^6 \equiv +1$ (mod. 13); 2 dagegen Nichtrest für 13, weil $2^6 \equiv -1$ (mod. 13) wird.

Sobald aber die zu untersuchenden Zahlen auch nur mässig gross sind, wird dieses Kennzeichen wegen des ungeheuren Umfanges der Rechnung völlig unbrauchbar.

§ 107. Es ist sehr leicht, bei vorgelegtem Modul alle Zahlen anzugeben, die für ihn Reste oder Nichtreste sind. Wird nämlich jene Primzahl gleich m gesetzt, so müssen die Quadrate bestimmt werden, deren Wurzeln $\frac{1}{2}m$ nicht überschreiten oder auch die, diesen Quadraten modulo m congruenten Zahlen für die Praxis giebt es noch bequemere

Methoden); dann werden alle Zahlen, die modulo m einer von jenen congruent sind, Reste für m; alle Zahlen aber, die keiner von jenen congruent sind, Nichtreste. — Die umgekehrte Aufgabe hingegen: alle Zahlen anzugeben, für die eine vorgelegte Zahl Rest oder Nichtrest ist, fordert weit tiefere Untersuchungen. Dieses Problem nun, von dessen Lösung das im Anfang des letzten Paragraphen dargelegte abhängt, wollen wir im Nachstehenden durchforschen und dabei mit den einfachsten Fällen beginnen.

Der Rest — 1.

§ 108. Lehrsatz. Für alle Primzahlen von der Form $4n+1$ ist -1 quadratischer Rest; für alle Primzahlen von der Form $4n+3$ ist -1 Nichtrest.

Beispiel. -1 ist Rest der Zahlen 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, ... für die Quadrate von 2, 5, 4, 12, 6, 9, 23, 11, 27, 34, 22, ..., hingegen Nichtrest für die Zahlen 3, 7, 11, 19, 23, 31, 43, 47, 59, 67, 71, 79, 83, ...

Der Beweis folgt leicht aus § 106. Denn für eine Primzahl der Form $4n+1$ ist $(-1)^{2n} \equiv 1$; für eine Primzahl der Form $4n+3$ hat man hingegen $(-1)^{2n+1} \equiv -1$. Wegen der Eleganz und der Brauchbarkeit dieses Satzes wird es nicht überflüssig sein, ihn noch auf eine andere Art zu beweisen.

§ 109. Wir wollen die Gesammtheit aller Reste der Primzahl p, welche kleiner als p sind, mit Ausschluss der Null, durch C bezeichnen. Da die Anzahl dieser Reste stets $= \frac{p-1}{2}$ wird, so ist sie offenbar für ein p von der Form $4n+1$ gerade, dagegen für ein p von der Form $4n+3$ ungerade. Nun nennen wir associirte Reste solche, deren Product $\equiv 1 \pmod{p}$ ist. Wenn nämlich r ein Rest ist, dann ist auch $\frac{1}{r} \pmod{p}$ ein Rest. Da nun kein Rest mehrere associirte Reste aus C haben kann, so können offenbar alle Reste C in Classen vertheilt werden, derart, dass eine jede zwei associirte Reste enthält. Giebt es nun keinen, sich selbst associirten Rest, d. h. enthält jede Classe zwei ungleiche Reste, so ist offenbar die Anzahl der Reste das Doppelte der Anzahl aller Classen; giebt es dagegen irgend welche sich selbst associirten Reste, d. h. Classen, welche

nur einen einzigen Rest, oder wenn man lieber will, denselben Rest zweimal enthalten, und wird die Anzahl dieser Classen gleich a, die der übrigen Classen gleich b gesetzt, dann wird die Anzahl aller Reste C gleich $a + 2b$. Ist also p von der Form $4n + 1$, dann wird a eine gerade Zahl; ist dagegen p von der Form $4n + 3$, dann wird a ungerade. Aber ausser 1 und $p - 1$ giebt es keine Zahlen, die kleiner als p und sich selbst associirt sind [denn es sind nur die Wurzeln der Congruenz $x^2 \equiv 1 \pmod{p}$]; nun kommt 1 sicher unter den Resten vor; im ersten Falle muss also $p - 1$ (oder, was hier dasselbe ist, -1) ein Rest sein, im zweiten ein Nichtrest; denn sonst würde in jenem Falle $a = 1$, in diesem jedoch $= 2$ werden, was unmöglich ist.

§ 111. Ist daher r Rest einer Primzahl von der Form $4n + 1$, dann wird auch $-r$ Rest dieser Primzahl sein; dagegen werden alle Nichtreste einer solchen Zahl auch bei geänderten Vorzeichen Nichtreste bleiben. Das Entgegengesetzte tritt für Primzahlen von der Form $4n + 3$ ein, deren Reste durch Aenderung des Vorzeichens zu Nichtresten werden, und umgekehrt. Uebrigens folgt aus dem Vorhergehenden leicht die allgemeine Regel: -1 ist Rest aller Zahlen, welche weder durch 4 noch durch irgend eine Primzahl von der Form $4n + 3$ getheilt werden können. Für alle übrigen Zahlen ist sie Nichtrest. Vergl. § 103 und 105.

Die Reste $+2$ und -2.

§ 112. Wir gehen zu den Resten $+2$ und -2 über. Unter den Primzahlen des ersten Hunderts finden sich folgende, deren Rest $+2$ ist: 7, 17, 23, 31, 41, 47, 71, 73, 79, 89, 97. Man bemerkt leicht, dass unter diesen Zahlen keine von der Form $8n + 3$ und $8n + 5$ vorkommt.

Wir wollen zusehen, ob man von dieser Induction zur Gewissheit gelangen kann.

Zunächst bemerken wir, dass jede zusammengesetzte Zahl von der Form $8n + 3$ oder $8n + 5$ nothwendiger Weise einen Primfactor von einer der Formen $8n + 3$ oder $8n + 5$ enthält; denn offenbar können aus Primzahlen von den Formen $8n + 1$, $8n + 7$ allein nur Zahlen von den Formen $8n + 1$ oder $8n + 7$ zusammengesetzt werden. Wenn daher unser Inductionsschluss allgemein gültig ist, so giebt es überhaupt

keine Zahl von der Form $8n + 3$, $8n + 5$, für welche $+ 2$ Rest ist; und somit giebt es sicher keine Zahl solcher Form im ersten Hundert, für welche $+ 2$ Rest ist. Gäbe es jenseits dieser Grenze solche Zahlen, so möge die kleinste unter ihnen $= t$ sein. Demnach ist t von einer der Formen $8n + 3$, $8n + 5$; und $+ 2$ ist Rest für t, aber Nichtrest für jede kleinere Zahl der gleichen Form. Wir setzen $2 \equiv a^2$ (mod. t) und können hierbei stets a ungerade und zugleich $< t$ annehmen; (denn a hat mindestens zwei positive Werthe $< t$, deren Summe gleich t und von denen also der eine gerade und der andere ungerade ist). Nun sei $a^2 = 2 + tu$ oder $tu = a^2 - 2$; dabei wird a^2 von der Form $8n + 1$, also tu von der Form $8n - 1$ und daher u von der Form $8n + 3$ oder $8n + 5$, je nachdem t von der zweiten oder von der ersten Form ist. Aus der Gleichung $a^2 = 2 + tu$ folgt, dass auch $2 \equiv a^2$ (mod. u), d. h. dass 2 auch für u Rest sei. Nun sieht man leicht, dass $u < t$ wird; folglich ist t nicht die kleinste, unserem Inductionssatze widersprechende Zahl. Demnach ist unser Inductionssatz allgemein richtig.

Verbindet man dies mit den Resultaten von § 111, so erhält man die folgenden Sätze:

I. Für alle Primzahlen der Form $8n + 3$ ist $+ 2$ Nichtrest und $- 2$ Rest.

II. Für alle Primzahlen der Form $8n + 5$ sind $+ 2$ und $- 2$ Nichtreste.

§ 113. Als Zahlen des ersten Hunderts, deren Rest $- 2$ ist, findet man 3, 11, 17, 19, 41, 43, 59, 67, 73, 83, 89, 97. Da es unter ihnen keine von den Formen $8n + 5$, $8n + 7$ giebt, so wollen wir versuchen, diesen Inductionsschluss zu einem allgemeinen Lehrsatze zu machen. Aehnlich wie im § 112 lässt sich zeigen, dass jede zusammengesetzte Zahl von der Form $8n + 5$ oder $8n + 7$ einen Primfactor der Form $8n + 5$ oder der Form $8n + 7$ enthalte, so dass, wenn unser Inductionssatz allgemein richtig ist, $- 2$ überhaupt nicht Rest irgend einer Zahl von der Form $8n + 5$ oder $8n + 7$ sein kann. Gäbe es jedoch solche Zahlen, so möge die kleinste unter ihnen $= t$ gesetzt werden, und es sei $- 2 = a^2 - tu$. Wird hier, wie oben, a ungerade und $< t$ angenommen, so wird u von der Form $8n + 5$ oder $8n + 7$, je nachdem t von der Form $8n + 7$ oder $8n + 5$ ist. Weil ferner $a^2 - 2 = tu$ und $a < t$ ist, so lässt sich leicht herleiten, dass auch $u < t$ wird. Daraus folgt endlich, dass $- 2$ für u Rest ist.

d. h. t wird, gegen die Annahme, nicht die kleinste Zahl, die unserem Inductionssatze widerspricht. Folglich ist -2 nothwendiger Weise Nichtrest aller Zahlen von einer der Formen $8n+5$, $8n+7$.

Verbindet man dies mit den Sätzen aus § 111, so entstehen folgende Theoreme:

I. Für alle Primzahlen von der Form $8n+5$ sind sowohl -2 wie $+2$ Nichtreste, was wir schon in § 112 gefunden haben.

II. Für alle Primzahlen von der Form $8n+7$ ist -2 Nichtrest, $+2$ hingegen Rest.

§ 114. Es bleibt noch der Fall zu behandeln übrig, dass die Primzahl von der Form $8n+1$ ist. Bei ihm versagt die vorige Methode, und es werden ganz besondere Kunstgriffe nöthig.

Für den Primzahlmodul $8n+1$ sei a irgend eine primitive Wurzel, und daher $a^{4n} \equiv -1$ (mod. $8n+1$). Diese Congruenz kann auch in die Formen $(a^{2n}+1)^2 \equiv 2a^{2n}$ oder $(a^{2n}-1)^2 \equiv -2a^{2n}$ mod. $8n+1$) gebracht werden. Daraus geht hervor, dass sowohl $2a^{2n}$ als $-2a^{2n}$ Reste für $8n+1$ sind. Da aber a^{2n} ein durch den Modul nicht theilbares Quadrat ist, so werden offenbar sowohl $+2$ wie -2 Reste sein.

§ 116. Uebrigens lässt sich aus dem Vorhergehenden leicht folgende Regel ableiten: $+2$ ist Rest jeder Zahl, welche weder durch 4 noch durch irgend eine Zahl der Form $8n+3$ oder $8n+5$ getheilt werden kann, Nichtrest dagegen von allen übrigen (z. B. von allen Zahlen einer der Formen $8n+3$, $8n+5$, gleichgültig ob sie Primzahlen sind oder zusammengesetzte Zahlen).

-2 ist Rest jeder Zahl, welche weder durch 4 noch durch irgend eine Primzahl der Form $8n+5$ oder $8n+7$ theilbar ist, Nichtrest dagegen von allen übrigen.

Die Reste $+3$ und -3.

§ 117. Wir gehen weiter zu den Resten $+3$ und -3 und beginnen mit dem letzten.

Im ersten Hundert giebt es folgende Primzahlen, deren Rest -3 ist: 3, 7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 97; unter ihnen kommt keine Zahl von der Form $6n+5$ vor. Dass es nun auch über diese Grenze hinaus keine Primzahl

von solcher Form giebt, deren Rest -3 ist, dies beweisen wir so: Zuerst ist es klar, dass jede zusammengesetzte Zahl der Form $6n+5$ nothwendiger Weise einen Primfactor derselben Form habe. So weit es also keine Primzahlen der Form $6n+5$ giebt, für die -3 Rest ist, so weit giebt es auch keine solchen zusammengesetzten Zahlen. Gäbe es über das erste Hundert hinaus derartige Zahlen, so sei die kleinste unter ihnen $= t$, und es werde $-3 = a^2 - tu$ gesetzt. Wir nehmen a als gerade und kleiner als t an; dann wird $u < t$ und -3 Rest von u. Ist nun a von der Form $6n \pm 2$, dann wird tu von der Form $6n+1$ und u folglich von der Form $6n+5$, was nicht angeht, da t als kleinste Zahl angenommen ist, die unserer Induction widerspricht. Ist jedoch a von der Form $6n$, dann wird tu von der Form $36n+3$ und somit $\frac{1}{3}tu$ von der Form $12n+1$; deshalb wird $\frac{1}{3}u$ von der Form $6n+5$. Es ist aber klar, dass -3 Rest für $\frac{1}{3}u$ wird, und dass $\frac{1}{3}u < t$ ist, was nicht angeht. Sonach liegt es auf der Hand, dass -3 für keine Zahl von der Form $6n+5$ ein Rest sein kann.

Da nun jede Zahl von der Form $6n+5$ nothwendig entweder unter der Form $12n+5$ oder unter der Form $12n+11$ enthalten ist, die erste aber unter $4n+1$ und die letzte unter $4n+3$, so gelten folgende Sätze:

I. Für jede Primzahl von der Form $12n+5$ sind -3 und $+3$ Nichtreste.

II. Für jede Primzahl von der Form $12n+11$ ist -3 Nichtrest und $+3$ Rest.

§ 118. Im ersten Hundert giebt es folgende Primzahlen, für welche $+3$ Rest ist: 3, 11, 13, 23, 37, 47, 59, 61, 71, 73, 83, 97; unter diesen kommt keine von einer der Formen $12n+5$ oder $12n+7$ vor. Dass es nun überhaupt keine Zahl einer der Formen $12n+5$, $12n+7$ giebt, für welche $+3$ Rest ist, das kann auf genau die, in § 112, 113, 117 benutzte Art bewiesen werden; deshalb übergehen wir es. Mit Hülfe von § 111 ergeben sich also folgende Sätze:

I. Für jede Primzahl von der Form $12n+5$ sind $+3$ und -3 Nichtreste (wie wir schon im vorigen Paragraphen gefunden haben).

II. Für jede Primzahl von der Form $12n+7$ ist $+3$ Rest und -3 Nichtrest.

§ 119. Ueber die Zahlen von der Form $12n+1$ lässt sich durch die angewendete Methode nichts feststellen; ihre

Untersuchung erfordert ganz besondere Kunstgriffe. Die Induction zeigt leicht, dass für alle Primzahlen dieser Form $+3$ und -3 Reste seien. Man braucht aber offenbar nur zu beweisen, -3 sei Rest für derartige Zahlen, weil dann nach § 111 auch $+3$ ein Rest sein muss. Wir werden den allgemeineren Satz herleiten, dass -3 Rest jeder Primzahl $3n+1$ ist.

p möge eine solche Zahl bedeuten, und a gehöre modulo p zum Exponenten 3; (solche Zahlen giebt es, weil 3 ein Theiler von $p-1$ ist). Dann wird $a^3 \equiv 1$ (mod. p), d. h. es wird a^3-1 oder $(a^2+a+1)(a-1)$ durch p theilbar. a kann nicht $\equiv 1$ mod. p sein, weil 1 zum Exponenten 1 gehört; deshalb wird nicht $a-1$, sondern a^2+a+1 durch p theilbar; folglich auch $4a^2+4a+4$, d. h. es wird $(2a+1)^2 \equiv -3$ (mod. p) oder -3 Rest für p, w. z. b. w.

Uebrigens ist es klar, dass dieser, vom Vorhergehenden unabhängige Beweis auch die im vorigen Paragraphen bereits erledigten Primzahlen der Form $12n+7$ umfasst.

§ 120. Aus dem Vorhergehenden folgen leicht die nachstehenden Sätze (vgl. § 102, 103, 105):

I. -3 ist Rest aller Zahlen, welche weder durch 8, noch durch 9, noch durch irgend eine Primzahl von der Form $6n+5$ getheilt werden können; Nichtrest dagegen von allen anderen Zahlen.

II. $+3$ ist Rest aller Zahlen, welche weder durch 4, noch durch 9, noch durch irgend eine Primzahl von der Form $12n+5$ oder $12n+7$ getheilt werden können, und Nichtrest aller übrigen.

Insbesondere merke man den folgenden Fall:

-3 ist Rest aller Primzahlen von der Form $3n+1$, oder, was dasselbe aussagt, aller Primzahlen, welche Reste von 3 sind, dagegen Nichtrest aller Primzahlen von der Form $6n+5$, oder, nach Ausschluss der Zahl 2, aller von der Form $3n+2$, d. h. aller, welche Nichtreste von 3 sind. Ferner erkennt man leicht, dass alle übrigen Fälle von selbst hieraus folgen.

Die Reste $+5$ und -5.

§ 121. Durch Induction kommt man darauf, dass $+5$ für keine ungerade Zahl der Form $5n+2$ oder $5n+3$ Rest ist, d. h. für keine ungerade Zahl, welche Nichtrest von 5 ist.

Dass diese Regel keine Ausnahme zulässt, wird so bewiesen. Wenn es Ausnahmen giebt, sei t die niedrigste Zahl unter denen, welche der Regel widersprechen, so dass t Nichtrest von 5, dagegen 5 Rest von t ist. Nun sei $a^2 = 5 + tu$, und dabei a gerade und kleiner als t. Dann wird u ungerade und kleiner als t, und 5 Rest von u. Ist nun a nicht durch 5 theilbar, so ist es auch u nicht; offenbar ist aber tu Rest von 5, und weil t Nichtrest von 5 ist, so ist auch u Nichtrest von 5, d. h. es giebt einen ungeraden Nichtrest für 5, für den 5 Rest ist und der gegen die Annahme $< t$ bleibt. Falls aber a durch 5 theilbar ist, setzen wir $a = 5b$ und $u = 5v$; daraus folgt $tv \equiv -1 \equiv 4$ (mod. 5), d. h. tv wird Rest von 5. Der Beweis geht nun ebenso weiter wie im ersten Falle.

§ 122. Es werden also für alle Primzahlen, die Nichtreste für 5 und zugleich von der Form $4n + 1$ sind, d. h. also für alle Primzahlen der Form $20n + 13$ oder $20n + 17$, sowohl $+ 5$ wie $- 5$ Nichtreste werden; für alle Primzahlen der Form $20n + 3$ oder $20n + 7$ dagegen wird $+ 5$ Nichtrest und $- 5$ Rest.

Auf ganz ähnliche Art lässt sich beweisen, dass $- 5$ Nichtrest aller Primzahlen von einer der Formen $20n + 11$, $20n + 13$, $20n + 17$, $20n + 19$ ist, und hieraus folgt leicht, dass $+ 5$ Rest aller Primzahlen von der Form $20n + 11$ oder $20n + 19$, dagegen Nichtrest aller von der Form $20n + 13$ oder $20n + 17$ wird. Und da jede Primzahl ausser 2 und 5, (für welche ± 5 Rest ist), in einer der Formen $20n + 1$, 3, 7, 9, 11, 13, 17, 19 enthalten ist, so lässt sich jetzt schon für alle Zahlen die Entscheidung liefern mit Ausnahme derjenigen, welche von der Form $20n + 1$ oder $20n + 9$ sind.

§ 123. Durch Induction kommt man leicht darauf, dass $+ 5$ und $- 5$ Reste aller Primzahlen der Form $20n + 1$ oder $20n + 9$ sind. Ist dies allgemein wahr, dann gilt der elegante Satz: $+ 5$ ist Rest aller Primzahlen, welche Reste von 5 sind (denn diese sind in einer der Formen $5n + 1$, $5n + 4$ oder auch in einer der Formen $20n + 1$, 9, 11, 19 enthalten, für deren dritte und vierte der Satz schon gezeigt ist); dagegen ist $+ 5$ Nichtrest aller ungeraden Zahlen, welche Nichtreste von 5 sind, wie wir oben schon bewiesen haben. Es ist nun klar, dass dies Theorem zur Bestimmung darüber ausreicht, ob $+ 5$ (und ebenso $- 5$,

welches als Product von $+5$ und -1 zu betrachten ist) Rest oder Nichtrest irgend welcher gegebenen Zahl sei. Endlich machen wir auf die Analogie aufmerksam, welche zwischen diesem Theoreme und dem in § 120 über den Rest -3 dargelegten besteht.

Die Bestätigung jenes Inductionssatzes ist nicht gerade leicht. Hat die vorgelegte Primzahl die Form $20n+1$ oder allgemeiner $5n+1$, dann lässt sich die Sache auf ähnliche Weise abthun, wie in § 114, 119. Es sei nämlich a irgend eine für den Modul $5n+1$ zum Exponenten 5 gehörige Zahl, dann wird $a^5 \equiv 1$ oder $(a-1)(a^4+a^3+a^2+a+1) \equiv 1$ (mod. $5n+1$). Weil nun $a \equiv 1$ und deshalb $a-1 \equiv 0$ unmöglich ist, so muss $a^4+a^3+a^2+a+1 \equiv 0$ sein. Daher wird auch $4(a^4+a^3+a^2+a+1) = (2a^2+a+2)^2 - 5a^2 \equiv 0$, d. h. $5a^2$ Rest von $5n+1$ werden, und deshalb auch 5, da a^2 ein, wegen $a^5 \equiv 1$ durch $5n+1$ nicht theilbarer Rest ist; w. z. b. w.

Dagegen erfordert der Fall, in welchem die vorgelegte Zahl die Form $5n+4$ hat, feinere Kunstgriffe. Da aber die Sätze, mit deren Hülfe sich unser Vorhaben erledigt, im Folgenden allgemeiner behandelt werden sollen, so brauchen wir sie hier nur leicht zu streifen.

I. Ist p eine Primzahl und b ein gegebener quadratischer Nichtrest von p, so wird der Werth des Ausdruckes

$$(A) \qquad \frac{(x+\sqrt{b})^{p+1} - (x-\sqrt{b})^{p+1}}{\sqrt{b}},$$

(aus dem, wie man leicht sieht, bei der Entwickelung die Irrationalität herausfällt) stets durch p theilbar sein, was für eine Zahl auch für x genommen wird. Denn aus der Betrachtung der, bei der Entwickelung von A auftretenden Coefficienten folgt, dass alle Glieder vom zweiten bis zum vorletzten incl. durch p theilbar sind; folglich wird

$$A \equiv 2(p+1)\left(x^p + x b^{\frac{p-1}{2}}\right) \text{ (mod. } p).$$

Da nun b Nichtrest von p ist, so wird

$$b^{\frac{p-1}{2}} \equiv -1 \text{ (mod. } p)$$

(§ 106); ferner ist x^p stets $\equiv x$, und also $A \equiv 0$; w. z. b. w.

II. In der Congruenz $A \equiv 0$ (mod. p) steigt die Unbestimmte x bis zum p^{ten} Grade auf, und alle Zahlen 0, 1, 2, ... $p - 1$ werden Wurzeln dieser Congruenz. Nun möge e ein Theiler von $p + 1$ sein, dann wird der Ausdruck

$$(B) \qquad \frac{(x + \sqrt{b})^e - (x - \sqrt{b})^e}{\sqrt{b}}$$

bei seiner Entwickelung von der Irrationalität frei; er steigt in x bis zum Grade $e - 1$; und A ist, wie aus den ersten Elementen der Algebra feststeht, durch B unbestimmt theilbar. Ich behaupte, dass es $e - 1$ Werthe von x giebt, durch deren Substitution in B dies durch p theilbar gemacht wird. Es werde nämlich $A \equiv BC$ gesetzt; x tritt in C im Grade $p - e + 1$ auf; folglich hat $C \equiv 0$ (mod. p) nicht mehr als $p - e + 1$ Wurzeln. Hieraus folgt leicht, dass alle übrigen Zahlen der Reihe 0, 1, 2, 3, ... $p - 1$, deren Anzahl [mindestens] gleich $e - 1$ ist, Wurzeln der Congruenz $B \equiv 0$ sein werden.

III. Nun nehmen wir an, p sei von der Form $5n + 4$, ferner $e = 5$, b ein Nichtrest von p, und a so bestimmt, dass

$$\frac{(a + \sqrt{b})^5 - (a - \sqrt{b})^5}{\sqrt{b}}$$

durch p theilbar wird. Es ist dieser Ausdruck aber

$$= 10a^4 + 20a^2b + 2b^2 = 2\left((b + 5a^2)^2 - 20a^4\right).$$

Folglich wird auch $(b + 5a^2)^2 - 20a^4$ durch p theilbar, d. h. $20a^4$ Rest von p. Demnach wird auch 5 Rest von p sein, da ja $4a^4$ ein durch p nicht theilbarer Rest ist; (denn man sieht leicht ein, dass a durch p nicht getheilt werden kann). W. z. b. w.

Hieraus folgt, dass das zu Anfang des Paragraphen aufgestellte Theorem allgemein richtig ist.

Vorbereitung zur allgemeinen Untersuchung.

§ 125. Da nun aber die vorhergehenden Methoden keine geeignete Grundlage eines allgemeinen Beweises abgeben, so ist es an der Zeit, einen von jenem Mangel freien Beweis darzulegen. Wir beginnen mit einem Theoreme, dessen Begründung lange Zeit unseren Bemühungen widerstanden hat,

obwohl es auf den ersten Blick so naheliegend erscheint, dass Mancher nicht einmal die Nothwendigkeit eines solchen Beweises einsehen möchte. Es ist folgendes Theorem: Abgesehen von den positiv genommenen Quadraten ist jede Zahl Nichtrest irgend welcher Primzahl. Da wir dieses Theorem aber nur als Hülfssatz bei anderen Beweisen benutzen werden, wollen wir hier nur diejenigen Fälle auseinandersetzen, deren wir zu jenem Zwecke bedürfen. Die übrigen Fälle erledigen sich dann von selbst. Wir wollen daher nur zeigen, dass jede positiv oder negativ genommene Primzahl von der Form $4n+1$ Nichtrest gewisser Primzahlen sei*) und zwar, wenn jene Primzahl > 5 ist, Nichtrest einer kleineren Primzahl.

Zuerst sei p eine Primzahl von der Form $4n+1$; (wir setzen sie > 17, trotzdem $-13\,N\,3$ und $-17\,N\,5$ ist**)); sie soll negativ genommen werden. Ist nun $2a$ die kleinste gerade Zahl, welche $\sqrt{p}$ übertrifft, dann erkennt man leicht, dass $4a^2$ immer $< 2p$ ist², oder $4a^2 - p < p$. Aber $4a^2 - p$ ist von der Form $4n+3$, und p quadratischer Rest von $4a^2 - p$, (weil ja $p \equiv 4a^2$ mod. $4a^2 - p$). Ist also $4a^2 - p$ eine Primzahl, so ist $-p$ Nichtrest für sie. Ist $4a^2 - p$ keine Primzahl, dann wird einer ihrer Primfactoren von der Form $4n+3$; und da $+p$ auch für ihn Rest ist, so wird $-p$ für ihn Nichtrest; w. z. b. w.

Bei positiv genommenen Primzahlen unterscheiden wir zwei Fälle. Zunächst sei p eine Primzahl von der Form $8n+5$, und a sei irgend eine positive Zahl $< \sqrt{\tfrac{1}{2}p}$. Dann wird $8n+5-2a^2$ eine positive Zahl der Form $8n+5$ oder $8n+3$ werden (je nachdem a gerade oder ungerade ist); folglich wird $8n+5-2a^2$ nothwendigerweise durch eine Primzahl von der Form $8n+3$ oder $8n+5$ theilbar; denn ein Product beliebig vieler Zahlen der Form $8n+1$ und $8n+7$ kann weder die Form $8n+3$ noch $8n+5$ haben. Dieser Primzahltheiler sei q; dann wird $8n+5 \equiv 2a^2$ (mod. q). Nun ist 2 Nichtrest von q (§ 112), folglich auch $2a^2$***) und $8n+5$; w. z. b. w.

*) Es ist von selbst klar, dass $+1$ auszunehmen ist.

**) [Die aus § 131 vorausgenommene Bezeichnung N bedeutet, dass die vorhergehende Zahl Nichtrest der folgenden ist.]

***) Nach § 98. Denn a^2 ist ein durch q nicht theilbarer Rest von q, weil sonst auch die Primzahl p durch q theilbar sein würde. W. z. b. w.

§ 126. Dass jede positiv genommene Primzahl von der Form $8n+1$ stets Nichtrest einer kleineren Primzahl sei, lässt sich durch so naheliegende Kunstgriffe nicht beweisen. Da jedoch die Richtigkeit dieses Satzes von grösstem Gewichte ist, so können wir seinen Beweis, wiewohl er etwas umständlich wird, doch nicht übergehen. Wir beginnen mit dem folgenden

Hülfssatz. Sind zwei Zahlenreihen vorgelegt

$$\text{(I)}\quad A, B, C, \ldots; \qquad \text{(II)}\quad A', B', C', \ldots,$$

bei denen es nichts ausmacht, ob sie gleiche oder ungleiche Gliederzahl besitzen, von der Eigenschaft, dass, wenn p irgend eine Primzahl oder Primzahlpotenz bedeutet, welche ein Glied oder auch mehrere Glieder der zweiten Reihe theilt, durch dieses p mindestens eben so viele Glieder der ersten Reihe theilbar werden wie der zweiten, dann ist das Product aller Zahlen (I) durch das Product aller Zahlen (II) theilbar.

Beispiel. (I) möge aus den Zahlen 12, 18, 45 bestehen; (II) aus 3, 4, 5, 6, 9. Dann werden durch 2, 4, 3, 9, 5 in (I) theilbar sein bezw. 2, 1, 3, 2, 1 Glieder und in (II) bezw. 2, 1, 3, 1, 1. Demnach ist das Product aller Glieder von (I), nämlich 9720 durch das Product aller Glieder von (II), nämlich 3240 theilbar.

Beweis. Das Product aller Glieder von (I) sei $=Q$, dasjenige aller Glieder der Reihe (II) $=Q'$. Dann ist es klar, dass jede Primzahl, welche Q' theilt, auch Q theilen wird. Nun wollen wir zeigen, dass jeder Primfactor von Q' mindestens in derselben Potenz in Q vorkommt wie in Q'. Es sei p ein solcher Theiler, und es mögen in (I) a Glieder durch p theilbar sein, b Glieder durch p^2, ebenso c Glieder durch p^3 u. s. w. Die Buchstaben $a', b', c', \ldots$ mögen das Entsprechende für die Reihe (II) bedeuten. Dann erkennt man leicht, dass p in Q in der Potenz $a+b+c+\ldots$ und in Q' in der Potenz $a'+b'+c'+\ldots$ auftritt. Nun ist a' sicher nicht grösser als a, b' nicht grösser als b, u. s. w. nach der Voraussetzung; folglich ist $a'+b'+c'+\ldots$ sicher nicht $>a+b+c+\ldots$ Da also keine Primzahl bei Q' in höherer Potenz eingeht als bei Q, so ist Q durch Q' theilbar, w. z. b. w.

§ 127. Hülfssatz. In der Reihe $1, 2, 3, 4, \ldots n$ können nicht mehr Glieder durch irgend welche Zahl h theilbar

sein, als in der aus eben so vielen Gliedern bestehenden $a, a+1, a+2, \ldots a+n-1$.

Man erkennt ohne Schwierigkeit, dass, wenn n ein Vielfaches von h ist, in beiden Reihen $\frac{n}{h}$ Glieder durch h theilbar werden; im anderen Falle setzen wir $n = eh + f$, wobei $f < h$ sein soll, dann werden in der ersten Reihe e Glieder durch h theilbar und in der zweiten entweder eben so viele oder $e+1$.

Eine Folgerung ist der aus der Theorie der figurirten Zahlen bekannte Satz, der aber bisher wohl von Niemanden direct bewiesen worden ist, dass

$$\frac{a(a+1)\cdot(a+2)\ldots(a+n-1)}{1\cdot 2\cdot 3\ldots n}$$

stets eine ganze Zahl wird.

Endlich merken wir an, dass man diesen Hülfssatz folgendermaassen allgemeiner hätte aufstellen können:

In der Reihe $a, a+1, a+2, \ldots a+n-1$ sind mindestens ebenso viele Glieder einer beliebigen Zahl r nach einem gegebenen Modul h congruent, wie in der Reihe $1, 2, 3, \ldots n$ durch h theilbar sind.[3])

§ 128. Lehrsatz. Ist a irgend eine Zahl von der Form $8n+1$, p irgend eine zu a theilerfremde Zahl, für welche $+a$ Rest ist, und endlich m eine beliebige Zahl, dann giebt es in der Reihe

$$a,\ \tfrac{1}{2}(a-1),\ 2(a-4),\ \tfrac{1}{2}(a-9),\ 2(a-16),\ \ldots\ \ldots 2(a-m^2) \text{ bezw. } \tfrac{1}{2}(a-m^2),$$

je nachdem m gerade oder ungerade ist, mindestens eben so viele durch p theilbare Glieder wie in der Reihe

$$1, 2, 3, \ldots\ 2m+1.$$

Die erste Reihe bezeichnen wir mit (I), die zweite mit (II).

Beweis. I. Ist $p=2$, dann sind in (I) alle Glieder mit Ausnahme des ersten, also m Glieder durch p theilbar; und eben so viele in (II). II. Es sei p eine ungerade, oder das Doppelte oder das Vierfache einer ungeraden Zahl*) und $a \equiv r^2 \pmod{p}$. Dann giebt es in der Reihe $-m, -(m-1), -(m-2), \ldots +m$ (welche mit (II) gleiche Gliederanzahl

---

*) [Hierunter ist auch $p=4$ enthalten.]

hat und mit (III) bezeichnet werden wird mindestens so viele Glieder $\equiv r$ (mod. p), als in (II) durch p theilbar sind (§ 127). Unter diesen können keine zwei vorkommen, welche nur durch ihr Vorzeichen aber nicht durch ihre Grösse sich unterscheiden*). Endlich entspricht jedem solchen Gliede ein anderes in (I), welches durch p theilbar wird. Ist nämlich $\pm b$ ein Glied aus (III), welches $\equiv r$ (mod. p) ist, dann muss $a - b^2$ durch p theilbar sein. Ist nun b gerade, so wird das Glied $2(a - b^2)$ der Reihe (I) durch p theilbar. Ist dagegen b ungerade, so wird das Glied $\frac{1}{2}(a - b^2)$ durch p theilbar; denn offenbar ist $\frac{a - b^2}{p}$ eine gerade ganze Zahl, weil $a - b^2$ durch 8, p dagegen höchstens durch 4 theilbar ist; (denn a ist nach der Voraussetzung von der Form $8n + 1$; ebenso wird b^2, als Quadrat einer ungeraden Zahl, von dieser Form sein, und die Differenz daher von der Form $8n$). Daraus folgt endlich, dass in der Reihe (I) eben so viele Glieder durch p theilbar sind, als in (III) $\equiv r$ (mod. p) werden, d. h. eben so viele oder mehr als in (II) durch p theilbar sind; w. z. b. w.

III. Ist p von der Form $8n$**), so sei $a \equiv r^2$ (mod. $2p$). Denn man erkennt leicht, dass a, welches nach der Voraussetzung Rest für p ist, auch Rest für $2p$ sein wird.[1] Dann sind in der Reihe (III) mindestens eben so viele Glieder $\equiv r$ (mod. p), als in (II) durch p theilbar sind, und alle diese sind ihrer absoluten Grösse nach verschieden. Jedem unter ihnen entspricht in (I) ein durch p theilbares Glied. Ist nämlich $+b$ oder $-b \equiv r$ (mod. p), dann wird $b^2 \equiv r^2$ (mod. $2p$)***), und folglich ist $\frac{1}{2}(a - b^2)$ durch p theilbar. Demnach giebt es in (I) mindestens so viele durch p theilbare Glieder wie in (II). W. z. b. w.

§ 129. Lehrsatz. Ist a eine Primzahl von der Form $8n + 1$, so giebt es nothwendiger Weise unterhalb $2\sqrt{a} + 1$ eine Primzahl, für die a Nichtrest ist.

*) Wäre nämlich $r \equiv f \equiv -f$ (mod. p), so würde $2f$ und also auch, weil $f^2 \equiv a$ (mod. p) ist, $2a$ durch p theilbar. Das ist nur für $p = 2$ möglich, da nach der Voraussetzung a theilerfremd zu p ist. Diesen Fall aber haben wir gesondert erledigt.

**) [Hierunter ist auch $p = 2^\nu$ bei $\nu > 2$ enthalten.]

***) Es ist nämlich $b^2 - r^2 = (b - r)(b + r)$ ein Product aus zwei Factoren, deren einer nach der Voraussetzung durch p, und deren anderer, da b und r ungerade sind, durch 2 theilbar ist. Folglich ist $b^2 - r^2$ durch $2p$ theilbar.

Beweis. Es sei, wenn dies möglich wäre, a Rest aller Primzahlen, die $< 2\sqrt{a} + 1$ sind. Dann sieht man leicht ein, dass a auch Rest aller zusammengesetzten Zahlen sein wird, die $< 2\sqrt{a} + 1$ sind (man vergleiche die Vorschriften, die wir gegeben haben, um zu entscheiden, ob eine vorgelegte Zahl Rest einer zusammengesetzten sei oder nicht, § 105). Nun sei m die höchste ganze Zahl, die $\sqrt{a}$ nicht übertrifft. Dann giebt es in der Reihe

$$\text{(I)} \qquad a,\ \tfrac{1}{2}(a-1),\ 2(a-4),\ \tfrac{1}{2}(a-9), \ldots \ldots 2(a-m^2) \text{ bezw. } \tfrac{1}{2}(a-m^2)$$

eben so viele oder mehr Glieder, welche durch irgend eine Zahl $< 2\sqrt{a} + 1$ theilbar sind, wie in der Reihe

$$\text{(II)} \qquad 1, 2, 3, 4, \ldots\ldots 2m+1 \quad (\S\ 128).$$

Hieraus folgt, dass das Product aller Glieder (I) durch dasjenige aller Glieder (II) theilbar wird (§ 126). Nun ist jenes $= a(a-1)(a-4)\ldots(a-m^2)$ bezw. die Hälfte dieses Productes, je nachdem m gerade oder ungerade ist. Deshalb ist sicher das Product $a(a-1)(a-4)\ldots(a-m^2)$ durch das Product aller Glieder von (II) theilbar, und ebenso jenes Product nach Weglassung von a, da alle Glieder von (II) zu a theilerfremd sind. Das Product aus allen Gliedern (II) kann auch so geschrieben werden:

$$(m+1)((m+1)^2-1)((m+1)^2-4)\ldots((m+1)^2-m^2).$$

Demnach wird

$$\frac{1}{m+1} \cdot \frac{a-1}{(m+1)^2-1} \cdot \frac{a-4}{(m+1)^2-4} \cdots \frac{a-m^2}{(m+1)^2-m^2}$$

eine ganze Zahl, obwohl es ein Product aus echten Brüchen ist: denn weil $\sqrt{a}$ irrational sein muss, so wird $m+1 > \sqrt{a}$ und $(m+1)^2 > a$. Hieraus endlich schliesst man, dass unsere Annahme nicht statt haben kann; w. z. b. w.

Weil a sicher > 9 ist, so wird $2\sqrt{a} + 1 < a$, und folglich giebt es eine Primzahl $< a$, für welche a Nichtrest ist.

Durch Induction wird man auf das allgemeine (Fundamental-)Theorem geführt und zieht Schlüsse aus ihm.

§ 130. Nachdem wir streng bewiesen haben, dass jede Primzahl von der Form $4n+1$ positiv oder negativ genommen

Nichtrest einer kleineren Primzahl sei, gehen wir nunmehr zur genaueren und allgemeineren Vergleichung von Primzahlen über, darauf hin, ob die eine Rest oder Nichtrest der anderen sei.

Mit aller Strenge haben wir oben bewiesen, dass — 3 und + 5 Reste oder Nichtreste aller Primzahlen werden, welche ihrerseits von 3 und von 5 Reste bezw. Nichtreste sind.

Dehnen wir die Induction aus, so finden wir, dass — 7, — 11, + 13, + 17, — 19, — 23, + 29, — 31, + 37, + 41, — 43, — 47, + 53, — 59, . . . Reste oder Nichtreste aller Primzahlen werden, welche für jene positiv genommenen Primzahlen bezw. Reste oder Nichtreste sind.

Eine leichte Aufmerksamkeit zeigt, dass diejenigen unter diesen Zahlen, welche die Form $4n + 1$ haben, mit positivem Vorzeichen, diejenigen hingegen, welche die Form $4n + 3$ haben, mit negativem Vorzeichen versehen vorkommen.

§ 131. Wir werden bald beweisen, dass diese Resultate der Induction allgemein gültig sind. Vorher wird es aber nöthig sein, Alles was aus jenem, als wahr angenommenen Theoreme folgt, herzuleiten. Das Theorem selbst wollen wir folgendermaassen aussprechen:

Ist p eine Primzahl von der Form $4n + 1$, dann wird $+ p$, ist dagegen p eine solche von der Form $4n + 3$, dann wird $- p$ Rest oder Nichtrest jeder Primzahl, welche positiv genommen für p Rest oder Nichtrest ist.

Weil sich fast alles, was über quadratische Reste ausgesagt werden kann, auf diesen Satz stützt, scheint die Bezeichnung Fundamentaltheorem, von der wir im Folgenden Gebrauch machen wollen, für ihn nicht unangebracht.

Um unsere Schlussfolgerungen so kurz wie möglich darlegen zu können, bezeichnen wir durch a, a', a'', . . . Primzahlen von der Form $4n + 1$; durch b, b', b'', . . . Primzahlen von der Form $4n + 3$; durch A, A', A'', . . . irgend welche Zahlen von der Form $4n + 1$; durch B, B', B'', . . . dagegen irgend welche Zahlen von der Form $4n + 3$; endlich soll der zwischen zwei Zahlen stehende Buchstabe R angeben, dass die erste Rest der zweiten sei, während der Buchstabe N die entgegengesetzte Bedeutung haben soll. Beispielsweise bezeichnet

$$+ 5 R 11, \quad \pm 2 N 5,$$

dass 5 Rest von 11 sei, und dass + 2 wie — 2 Nichtreste von 5 sind.

Verbindet man mit dem Fundamentaltheorem die Sätze von § 111, so ergeben sich leicht die folgenden Sätze[5])

	Wenn:		dann ist:
1.	$\pm a R a'$	·······	$\pm a' R a$
2.	$\pm a N a'$	·······	$\pm a' N a$
3.	$\left\{\begin{matrix} + a R b \\ - a N b \end{matrix}\right\}$	·······	$\pm b R a$
4.	$\left\{\begin{matrix} + a N b \\ - a R b \end{matrix}\right\}$	·······	$\pm b N a$
5.	$\pm b R a$	·······	$\left\{\begin{matrix} + a R b \\ - a N b \end{matrix}\right.$
6.	$\pm b N a$	·······	$\left\{\begin{matrix} + a N b \\ - a R b \end{matrix}\right.$
7.	$\left\{\begin{matrix} + b R b' \\ - b N b' \end{matrix}\right\}$	·······	$\left\{\begin{matrix} + b' N b \\ - b' R b \end{matrix}\right.$
8.	$\left\{\begin{matrix} + b N b' \\ - b R b' \end{matrix}\right\}$	·······	$\left\{\begin{matrix} + b' R b \\ - b' N b. \end{matrix}\right.$

§ 132. Hierunter sind alle Fälle enthalten, welche bei der Vergleichung zweier Primzahlen auftreten können. Die folgenden Formeln, deren Beweise weniger nahe liegen, beziehen sich auf irgend welche Zahlen.

	Wenn:		dann ist:
9.	$\pm a R A$	·······	$\pm A R a$
10.	$\pm b R A$	·······	$\left\{\begin{matrix} + A R b \\ - A N b \end{matrix}\right.$
11.	$+ a R B$	·······	$\pm B R a$
12.	$- a R B$	·······	$\pm B N a$
13.	$+ b R B$	·······	$\left\{\begin{matrix} - B R b \\ + B N b \end{matrix}\right.$
14.	$- b R B$	·······	$\left\{\begin{matrix} + B R b \\ - B N a. \end{matrix}\right.$

Da die Beweise aller dieser Behauptungen aus denselben Principien geschöpft werden können, so wird es nicht nöthig sein, alle zu entwickeln. Der Beweis der aufgestellten Behauptung 9. kann als Beispiel dienen. Vor allem möge bemerkt werden, dass jede Zahl von der Form $4n + 1$ entweder keinen Primfactor von der Form $4n + 3$ hat, oder 2 oder 4, ...; d. h. dass die Anzahl solcher Factoren (unter denen einander gleiche sein können), stets gerade ist; dass dagegen jede Zahl

von der Form $4n+3$ eine ungerade Anzahl von Primfactoren der Form $4n+3$ enthält (d. h. einen oder drei oder fünf u. s. w.). Die Anzahl der Primfactoren von der Form $4n+1$ bleibt unbestimmt.

Die Behauptung 9. wird folgendermaassen bewiesen. Ist A das Product aus den Primfactoren a', a'', a''', ...; b, b', b'', ..., so ist die Anzahl der Factoren b, b', b'', ... gerade (es ist auch möglich, dass gar keine vorkommen, was auf das Gleiche hinausläuft). Ist nun aRA, so ist a auch Rest aller Factoren a', a'', a''', ...; b, b', b'', ..., und daher werden nach § 131 Formeln 1., 3. diese einzelnen Factoren Reste von a, und deshalb wird es auch ihr Product A. Für $-A$ gilt dann das Gleiche. — Wenn jedoch $-aRA$ ist, und deshalb $-a$ auch Rest aller Factoren a', a'', ...; b, b', ..., dann werden die einzelnen a', a'', ... Reste von a, die einzelnen b, b' ... hingegen Nichtreste. Da aber die Anzahl der letzten Art gerade ist, so ist das Product aus ihnen allen, nämlich A Rest von a; und deswegen ist auch $-A$ Rest.

§ 133. Wir stellen eine noch allgemeinere Untersuchung an. Wir wollen zwei beliebige ungerade, theilerfremde, mit irgend welchen Vorzeichen versehene Zahlen P und Q betrachten. P möge ohne Rücksicht auf sein Vorzeichen in Primfactoren zerlegt sein; dann wollen wir durch p bezeichnen, für wie viele unter ihnen Q Nichtrest ist. Wenn dabei irgend eine Primzahl, deren Nichtrest Q ist, mehrfach unter den Factoren von P vorkommt, dann ist er so oft zu zählen, wie er vorkommt. Aehnlich sei q die Anzahl der Primfactoren von Q, für welche P Nichtrest ist. Dann besteht zwischen den Zahlen p, q eine gewisse gegenseitige Beziehung, die von der Beschaffenheit der Zahlen P, Q abhängt. Ist nämlich die eine der beiden Zahlen p, q gerade oder ungerade, dann lehrt die Form der Zahlen P, Q, ob die andere gerade oder ungerade sei. Diese Beziehung wird in der folgenden Tabelle angegeben.

Die Zahlen p, q werden zugleich gerade oder zugleich ungerade, wenn die Zahlen P, Q die Formen haben:

1. $+A$, $+A'$	4. $+A$, $-B$
2. $+A$, $-A'$	5. $-A$, $-A'$
3. $+A$, $+B$	6. $+B$, $-B'$.

Hingegen wird die eine der Zahlen p, q gerade und die andere ungerade, wenn die Zahlen P, Q die Formen haben:

7. $-A$, $+B$ 9. $+B$, $+B'$
8. $-A$, $-B$ 10. $-B$, $-B'$ *)

Beispiel. Es mögen die Zahlen -55 und $+1197$ vorgelegt sein: sie stehen unter dem vierten Falle. Es ist 1197 Nichtrest eines Primfactors von 55, nämlich des Factors 5; und -55 ist Nichtrest dreier Primfactoren von 1197, nämlich von 3, 3, 19.

Bezeichnen P und Q Primzahlen, dann gehen die aufgestellten Sätze in die § 131 behandelten über. Hierbei können nämlich p und q nicht grösser als 1 werden, und deshalb wird p, wenn es gerade sein muss, nothwendig $= 0$, d. h. Q wird Rest von P; wenn dagegen p ungerade ist, dann wird Q Nichtrest von P; und umgekehrt. Beispielsweise folgt, wenn man a, b statt A, B schreibt, aus 8., dass, wenn $-a$ Rest oder Nichtrest von b ist, dann $-b$ Nichtrest oder Rest von a wird, was mit 3. und 4. aus § 131 übereinstimmt.

Allgemein erkennt man, dass Q nur Rest von P sein kann, wenn $p = 0$ ist; bei ungeradem p ist also Q sicher Nichtrest von P.

Hieraus können auch die Angaben des vorigen Paragraphen ohne Schwierigkeit abgeleitet werden.

Es wird sich übrigens bald zeigen, dass diese allgemeine Darstellung mehr ist als eine unfruchtbare Speculation: der vollständige Beweis des Fundamentaltheorems möchte ohne sie kaum durchgeführt werden können.

§ 134. Wir gehen jetzt zur Herleitung dieser Sätze über.

I. Wie oben denken wir uns P in seine Primfactoren unter Vernachlässigung der Vorzeichen zerlegt; ausserdem möge Q auf irgend welche Weise in Factoren zerlegt sein, jedoch so, dass dem Zeichen von Q Rechnung getragen wird. Jene einzelnen Factoren mögen dann mit diesen einzelnen combinirt werden. Bezeichnet nun s die Anzahl aller Combinationen, in welchen der Factor von Q Nichtrest des Factors von P ist, dann werden p und s zugleich gerade und zugleich ungerade werden. Bezeichnen wir nämlich die Primfactoren von P mit $f, f', f'', \ldots$, so mögen unter den Factoren, in welche Q zerlegt ist, m sein, welche Nichtreste von f sind;

*) Setzt man $l = 1$, wenn beide Zahlen $P, Q \equiv 3$ (mod. 4) sind, und sonst $l = 0$; setzt man $m = 1$, wenn beide Zahlen P, Q negativ sind, und sonst $m = 0$, dann hängt jene Beziehung von $l + m$ ab.

m', welche Nichtreste von f' sind: m'', welche Nichtreste von f'' sind, u. s. w. Dann erkennt man leicht, dass

$$s = m + m' + m'' + \cdots$$

ist, und dass p angiebt, wie viele der Zahlen $m, m', m'', \ldots$ ungerade sind. Hieraus folgt sofort, dass bei geradem p auch s gerade ist, bei ungeradem p dagegen ungerade.

II. Dies gilt allgemein, auf welche Weise Q auch in Factoren zerlegt sei. Wir gehen nun zu besonderen Fällen über. Zuerst wollen wir den Fall betrachten, in welchem die eine der beiden Zahlen, nämlich P positiv ist, die andere dagegen, nämlich Q von der Form $+A$ oder der Form $-B$. Jetzt mögen P und Q in ihre Primfactoren zerlegt werden; dabei geben wir den einzelnen Factoren von P das positive Zeichen, den einzelnen Factoren von Q dagegen das positive oder das negative, je nachdem sie von der Form a oder b sind. Hierbei erhält, wie dies verlangt wurde, Q die Form $+A$ oder $-B$. Nun combiniren wir die einzelnen Factoren von P mit den einzelnen Factoren von Q; wie vorher bezeichne s die Anzahl der Combinationen, in denen der Factor von Q Nichtrest des Factors von P ist, und ähnlich bezeichne t die Anzahl der Combinationen, in denen der Factor von P Nichtrest des Factors von Q ist. Aus dem Fundamentaltheoreme folgt, dass jene Combinationen mit diesen identisch sind, und dass daher $s = t$ wird. Endlich ergiebt sich aus dem oben Bewiesenen $p \equiv s$ (mod. 2), $q \equiv t$ (mod. 2) und also $p \equiv q$ (mod. 2).

So hat man die Sätze 1., 3., 4. und 6. aus § 133.

Die übrigen Sätze können durch eine ähnliche Methode direct hergeleitet werden; doch fordert das eine neue Betrachtung, und es ist leichter, sie aus dem Vorhergehenden auf die folgende Art abzuleiten.

III. Wieder mögen P, Q zwei beliebige ungerade, theilerfremde Zahlen bezeichnen, und p, q die Anzahl der Primfactoren von P, Q, für welche Q bezw. P Nichtreste sind. Endlich sei p' die Anzahl derjenigen Primfactoren von P, für welche $-Q$ Nichtrest ist; (natürlich bedeutet $-Q$ eine positive Zahl, wenn Q negativ ist). Alle Primfactoren von P können in vier Classen vertheilt werden:

1) In Factoren der Form a, für welche Q Rest ist.
2) In Factoren der Form b, für welche Q Rest ist. Ihre Anzahl sei χ.

3. In Factoren der Form a, für welche Q Nichtrest ist. Ihre Anzahl sei ϑ.
4. In Factoren der Form b, für welche Q Nichtrest ist. Ihre Anzahl sei ω.

Dann erkennt man leicht, dass $p = \vartheta + \omega$, $p' = \chi + \vartheta$ sei.

Ist nun P von der Form $\pm A$, dann wird $\chi + \omega$ eine gerade Zahl und also auch $\chi - \omega$; deshalb wird

$$p' = p + \chi - \omega \equiv p \pmod{2}.$$

Ist dagegen P von der Form $\pm B$, dann zeigen ähnliche Schlüsse, dass p und p' modulo 2 incongruent sind.

IV. Diese Resultate wenden wir auf die einzelnen Fälle an. Zunächst mögen P und Q von der Form $+A$ sein; nach 1. wird dann $p \equiv q \pmod{2}$; nun ist auch $p' \equiv p \pmod{2}$, und deswegen $p' \equiv q \pmod{2}$. Das bestätigt die Behauptung 2.

Aehnlich wird, wenn P von der Form $-A$ und Q von der Form $+A$ ist, nach dem eben bewiesenen Satze 2. jetzt $p \equiv q \pmod{2}$, und daher wird wegen $p' \equiv p$ auch $p' \equiv q$. So ist auch 5. bewiesen.

Auf dieselbe Weise wird 7. aus 3. abgeleitet: 8. entweder aus 4. oder aus 7.; weiter 9. aus 6., und 10. gleichfalls aus 6.

Strenger Beweis des Fundamentaltheorems.

§ 135. Durch den vorhergehenden Paragraphen sind die Sätze aus § 133 zwar nicht bewiesen, aber es ist gezeigt worden, dass ihre Richtigkeit von derjenigen des Fundamentaltheorems abhängt, welches wir eine Zeit lang als wahr vorausgesetzt haben. Aber aus der Methode der Herleitung ist es offenbar, dass jene Sätze für zwei Zahlen P und Q gelten, sobald das Fundamentaltheorem für alle mit einander combinirten Primfactoren dieser Zahlen Geltung hat, sogar wenn es nicht allgemein wahr ist. Indem wir jetzt zum Beweise des Fundamentaltheorems selbst übergehen, schicken wir folgende Definition voraus:

Wir sagen, das Fundamentaltheorem sei bis zu einer Zahl M hin richtig, wenn es für irgend zwei Primzahlen gilt, von denen keine M übertrifft.

In ähnlicher Weise muss es verstanden werden, wenn wir sagen, die Sätze aus § 131, 132, 133 seien bis zu einer gewissen Grenze hin richtig. Man sieht leicht ein, dass, wenn die Richtigkeit des Fundamentaltheorems bis zu einer gewissen

Grenze hin feststeht, diese Sätze bis zu derselben Grenze hin Gültigkeit besitzen.

§ 136. Durch Induction kann man leicht feststellen, dass das Fundamentaltheorem für kleine Zahlen wahr sei; und so lässt sich eine Grenze bestimmen, bis zu welcher es sicher Geltung hat. Wir nehmen an, dass diese Induction angestellt sei; wie weit wir in ihr vorgegangen sind, ist völlig gleichgültig; ja, es würde genügen, wenn wir es nur bis zur Zahl 5 bestätigt gefunden hätten; und dies könnte durch die eine Bemerkung erledigt werden, dass $+5N3$, $\pm 3N5$ ist.

Wäre das Fundamentaltheorem nicht allgemein richtig, dann müsste es eine Grenze T geben, bis zu welcher es gilt, während es bis zur nächst höheren Zahl $T+1$ nicht mehr gälte. Dies aber heisst nichts anderes als: es sind zwei Primzahlen gegeben, deren grössere $T+1$ ist, und welche mit einander combinirt dem Fundamentaltheoreme sich widersprechend verhalten, während alle beliebigen anderen, zu je zwei genommenen Primzahlen, falls sie nur beide kleiner bleiben als $T+1$, dem Fundamentaltheorem unterworfen sind. Hieraus folgt, dass die Sätze aus § 131, 132, 133 bis zu T gleichfalls statt haben werden. Wir wollen jetzt zeigen, dass diese Annahme einer Grenze nicht bestehen kann. Es kann sowohl $T+1$ verschiedene Formen besitzen als auch die kleinere Primzahl, die mit $T+1$ combinirt unserer Annahme nach dem Fundamentaltheoreme widerspricht; dieser Verschiedenheit gemäss sind folgende Fälle zu unterscheiden. Jene Primzahl bezeichnen wir mit p.

Haben $T+1$ und p die Form $4n+1$, dann könnte das Fundamentaltheorem auf zweifache Weise falsch sein, wenn nämlich zugleich wäre

entweder $\pm pR(T+1)$ und $\pm (T+1)Np$;
oder zugleich $\pm pN(T+1)$ und $\pm (T+1)Rp$.

Haben $T+1$ und p die Form $4n+3$, dann wird das Fundamentaltheorem falsch, wenn man zugleich hat

entweder $+pR(T+1)$ und $-(T+1)Np$,
(oder was das Gleiche ist
$-pN(T+1)$ und $+(T+1)Rp$);
oder $+pN(T+1)$ und $-(T+1)Rp$,
(oder $-pR(T+1)$ und $+(T+1)Np$).

Hat $T+1$ die Form $4n+1$, und p die Form $4n+3$, dann wird das Fundamentaltheorem falsch, wenn man zugleich hat entweder

$$\pm pR(T+1) \text{ und } +(T+1)Np \text{ (oder } -(T+1)Rp\text{)};$$

oder

$$\pm pN(T+1) \text{ und } -(T+1)Np \text{ (oder } +(T+1)Rp\text{)}.$$

Hat $T+1$ die Form $4n+3$, und p die Form $4n+1$, dann wird das Fundamentaltheorem falsch, wenn man zugleich hat entweder

$$+pR(T+1) \text{ (oder } -pN(T+1)\text{) und } \pm(T+1)Np;$$

oder

$$+pN(T+1) \text{ (oder } -pR(T+1)\text{) und } \pm(T+1)Rp.$$

Könnte bewiesen werden, dass keiner dieser acht Fälle eintreten kann, dann wäre zugleich die Sicherheit dafür gegeben, dass die Richtigkeit des Fundamentaltheorems an keine obere Grenze gebunden ist. An diesen Nachweis treten wir jetzt heran; weil aber einige der Fälle von anderen abhängig sind, so lässt sich die Ordnung, in welcher sie aufgezählt worden sind, nicht beibehalten.

§ 137. Erster Fall. Wenn $T+1=a$ von der Form $4n+1$ ist, und p von derselben Form; wenn ferner $\pm pRa$ ist, dann kann nicht $\pm aNp$ sein. Dieser Fall war oben der erste.

Es sei $+p \equiv e^2$ mod. a; dabei werde, was stets erreicht werden kann, e gerade und $< a$ angenommen. Zwei Fälle sind zu unterscheiden.

I. e ist durch p nicht theilbar. Wir setzen $e^2 = p + af$; dann wird f positiv*) und von der Form $4n+3$ (d. h. von der Form B), $< a$ und durch p nicht theilbar. Ferner ist $e^2 \equiv p$ mod. f, d. h. pRf und deshalb $\pm fRp$ nach § 132, II (dieser Satz hat wegen $p, f < a$ Geltung). Nun ist auch $afRp$, und deshalb endlich $\pm aRp$.

II. Ist e durch p theilbar, dann sei

$$e = gp \text{ und } e^2 = p + aph, \text{ d. h. } pg^2 = 1 + ah.$$

Es wird h von der Form $4n+3$ oder B, und zu p und g^2

*) Da $p < a$ ist, würde $p - af$ bei positivem f eine negative Grösse werden und könnte also nicht $= e^2$ sein.

theilerfremd. Ferner wird pg^2Rh, deshalb auch pRh, und daher (§ 132, 11.) $\pm hRp$. Nun ist auch $\pm ahRp$, weil $-ah \equiv 1$ (mod. p) ist; deswegen wird $\pm aRp$.

§ 138. Zweiter Fall. Wenn $T+1 = a$ von der Form $4n+1$ ist, und p von der Form $4n+3$; wenn ferner $\pm pR(T+1)$, dann kann weder $+(T+1)Np$ noch $-(T+1)Rp$ sein. (Dieser Fall war oben der fünfte.)

Es sei wie oben $e^2 = p + fa$; dabei werde e gerade und $< a$ angenommen.

I. Wenn e durch p nicht theilbar ist, dann ist auch f durch p nicht theilbar; ausserdem wird f positiv, von der Form $4n+1$ (oder A) und $< a$; weiter ist $+pRf$, und folglich (§ 132, 10.) auch $+fRp$. Weil aber zugleich $+faRp$ ist, so wird $+aRp$ und auch $-aNp$.

II. Ist e durch p theilbar, dann sei $e = pg$ und $f = ph$. Daher ist $g^2p = 1 + ha$. Hierbei wird h positiv, von der Form $4n+3$ (oder B) und theilerfremd zu p und g^2. Ferner hat man $+g^2pRh$ und also $+pRh$. Daraus entnimmt man (§ 132, 13.) $-hRp$. Nun ist $-ahRp$, und daher $+aRp$ und $-aNp$.

§ 139. Dritter Fall. Wenn $T+1 = a$ von der Form $4n+1$ ist, und p von derselben Form; wenn ferner $\pm pNa$, dann kann nicht $\pm aRp$ sein. (Dieser Fall war oben der zweite.)

Wir bestimmen irgend eine Primzahl, die kleiner als a, und für welche $+a$ Nichtrest ist. Dass es solche gebe, haben wir oben (§ 125, 129) bewiesen. Hier sind aber zwei Fälle getrennt zu betrachten, je nachdem nämlich diese Primzahl von der Form $4n+1$ oder $4n+3$ ist; denn es ist nicht bewiesen worden, dass es derartige Primzahlen von jeder der beiden Formen giebt.

I. Es sei diese Primzahl von der Form $4n+1$; sie werde $= a'$ gesetzt. Dann wird (§ 137*) $\pm aNa'$ und also $\pm a'pRa$. Wir können daher $e^2 \equiv a'p$ (mod. a) setzen und e als gerade und $< a$ annehmen. Hier sind wieder vier Fälle zu unterscheiden.

1) Es ist e weder durch p noch durch a' theilbar. Wir setzen $e^2 = a'p \pm af$, wobei wir das Vorzeichen so wählen,

* [In *Gauss'* Werken I. p. 107. Z. 15 findet sich der störende Druckfehler: § 131. — Der Annahme nach ist aNa', dann kann nicht $\pm a'Ra$ sein, weil daraus nach § 137 folgen würde $\pm aRa'$.]

dass f positiv wird. Dann ist $f < a$, theilerfremd zu a' und p und besitzt für das obere Zeichen die Form $4n + 3$ und für das untere die Form $4n + 1$. Der Kürze wegen wollen wir nun die Anzahl der Primfactoren von y, für die x Nichtrest ist, mit $[x, y]$ bezeichnen. Dann wird $a'pRf$, und also $[a'p, f] = 0$. Folglich wird (nach § 133, 1 und 3.) $[f, a'p]$ eine gerade Zahl und daher entweder 0 oder 2. Folglich wird f Rest entweder von beiden Zahlen a' und p oder von keiner. Der erste Fall ist unmöglich. Denn $\pm af$ ist Rest von a', und ferner ist $\pm aNa'$ nach der Voraussetzung, so dass $\pm fNa'$ wird. Deshalb muss f Nichtrest für beide Zahlen a' und p sein. Wegen $\pm afRp$ wird dann $\pm aNp$; w. z. b. w.

2) Ist e zwar durch p aber nicht durch a' theilbar, dann sei $e = gp$ und $g^2p = a' \pm ah$, wobei das Vorzeichen so bestimmt sein möge, dass h positiv wird. Dann ist $h < a$, theilerfremd zu a', g, p und h besitzt für das obere Zeichen die Form $4n + 3$ und für das untere die Form $4n + 1$. Aus der mit p und mit a' bezw. multiplicirten Gleichung

$$g^2p = a' \pm ah$$

kann man ohne Schwierigkeit herleiten

$$(\alpha) \ldots pa'Rh; \quad (\beta) \ldots \pm ahpRa'; \quad (\gamma) \ldots aa'hRp.$$

Aus (α) folgt $[pa', h] = 0$ und deshalb nach § 133, 1. und 3.) $[h, pa'] \equiv 0$ mod. 2, d. h. h wird Nichtrest entweder von p und a' zugleich oder von keiner der beiden Grössen. Im ersten Falle folgt aus (β), dass $\pm apNa'$ ist, und da man nach der Voraussetzung $\pm aNa'$ hat, auch $\pm pRa'$. Hieraus schliesst man nach dem Fundamentaltheorem, welches ja für die Zahlen p, a' gilt, die kleiner als $T + 1$ sind, dass $\pm a'Rp$ werde. Dies und der Umstand, dass nach der Voraussetzung hNp ist, führt (γ) in $\pm aNp$ über, w. z. b. w. Im zweiten Falle ergiebt sich aus (β) $\pm apRa'$, hieraus $\pm pNa'$, $\pm a'Np$. Dies und der Umstand, dass hRp ist, liefert aus (γ) $\pm aNp$; w. z. b. w.

3) e ist durch a', aber nicht durch p theilbar. Für diesen Fall weicht der Beweis nur so wenig von dem des vorigen Falles ab, dass er wohl Niemandem Aufenthalt verursachen wird, der jenen begriffen hat*).

4) Es sei e sowohl durch a' als durch p theilbar und also auch durch $a'p$ (denn wir setzen die Zahlen a', p als

*) Hier tritt § 138 an die Stelle des § 137.

ungleich voraus, weil sonst der gewünschte Beweis dafür, dass aNp sei, schon in der Annahme aNa' enthalten wäre. Dann sei $e = ga'p$ und $g^2a'p = 1 \pm ah$. Nun wird $h < a$, zu a' und p theilerfremd und für das obere Zeichen von der Form $4n+3$, für das untere von der Form $4n+1$. Man erkennt leicht, dass aus jener Gleichung folgt

$$(\alpha) \ldots\ldots a'pRh; \quad (\beta) \ldots\ldots \pm ahRa'; \quad (\gamma) \ldots\ldots \pm ahRp$$

Aus diesem (α), welches mit dem α in 2) übereinstimmt, folgt genau wie dort, dass entweder zugleich hRp, hRa' oder zugleich hNp, hNa' wird. Im ersten Falle würde wegen (β) gegen die Voraussetzung aRa'; deshalb muss hNp sein; und aus (γ) folgt dann aNp.

II. Ist jene Primzahl von der Form $4n+3$, so wird der Beweis dem vorhergehenden so ähnlich, dass es uns überflüssig erscheint, ihn herzusetzen. Für diejenigen, welche ihn — was wir dringend empfehlen — für sich entwickeln wollen, bemerken wir nur, dass es nach der Aufstellung einer Gleichung von der Gestalt $e^2 = bp \pm af$ (in welcher b jene Primzahl bezeichnet) zur Durchsichtigkeit beitragen wird, wenn man jedes der beiden Zeichen für sich behandelt.

§ 140. Vierter Fall. Wenn $T+1 = a$ von der Form $4n+1$ ist, und p von der Form $4n+3$; wenn ferner $\pm pNa$, dann kann weder $+aRp$ noch $-aNp$ sein. (Dieser Fall war oben der sechste.)

Der Kürze wegen lassen wir auch den Beweis dieses Falles aus, welcher dem des dritten Falles durchaus ähnlich verläuft.

§ 141. Fünfter Fall. Wenn $T+1 = b$ von der Form $4n+3$ ist, und p von derselben Form; wenn ferner $+pRb$ oder $-pNb$, dann kann weder $+bRp$ noch $-bNp$ sein. (Dieser Fall war oben der dritte.)

Es sei $p \equiv e^2$ mod. b, und dabei e gerade und $< b$.

I. Ist e nicht durch p theilbar, dann sei $e^2 = p + bf$; dann wird f positiv, von der Form $4n+3$, $< b$ und zu p theilerfremd. Ferner wird pRf, und nach § 132, 13 dann $-fRp$. Hieraus und aus $bfRp$ entsteht $-bRp$ und also $+bNp$; w. z. b. w.

II. Ist e durch p theilbar, dann sei $e = pg$ und $g^2p = 1 + bh$. Dabei ist h von der Form $4n+1$ und zu p theilerfremd. Aus $p \equiv g^2p^2$ mod b folgt pRb und daraus (§ 132, 10)

$+hRp$; dies liefert in Verbindung mit $-bhRp$ endlich $-bRp$ und $+bNp$. W. z. b. w.

§ 142. Sechster Fall. Wenn $T+1=b$ von der Form $4n+3$ ist, und p von der Form $4n+1$, wenn ferner pRb, dann kann nicht $\pm bNp$ sein. (Dieser Fall war oben der siebente.)

Wir übergehen den Beweis, welcher dem vorhergehenden durchaus ähnlich verläuft.

§ 143. Siebenter Fall. Wenn $T+1=b$ von der Form $4n+3$ ist, und p von derselben Form; wenn ferner $+pNb$ oder $-pRb$, dann kann weder $+bNp$ noch $-bRp$ sein. (Dieser Fall war oben der vierte.)

Es sei $-p \equiv e^2$ (mod. b); e sei gerade und $< b$.

I. Ist e nicht durch p theilbar, dann sei $-p = e^2 - bf$; dabei wird f positiv, von der Form $4n+1$, zu p theilerfremd und $< b$ (denn e ist sicher nicht grösser als $b-1$, $p < b-1$ und daher wird $bf = e^2 + p < b^2 - b$, d. h. $f < b-1$). Ferner wird $-pRf$, hieraus (§ 132, 10.) $+fRp$, und demnach wegen $bfRp$ auch bRp oder $-bNp$.

II. Ist e durch p theilbar, so sei

$$e = pg \text{ und } g^2p = -1 + bh.$$

Dabei wird h positiv, von der Form $4n+3$, theilerfremd zu p und $< b$. Ferner wird $-pRh$, hieraus (§ 132, 11.) $+hRp$, und demnach wegen $bhRp$ auch bRp und $-bNp$. W. z. b. w.

§ 144. Achter Fall. Wenn $T+1=b$ von der Form $4n+3$ ist, und p von der Form $4n+1$; wenn ferner $+pNb$ oder $-pRb$, dann kann nicht $\pm bRp$ sein. (Dieser Fall war oben der letzte.)

Der Beweis nimmt genau den Weg, der im vorhergehenden Falle eingeschlagen wurde.[6]

Durch eine entsprechende Methode werden die Sätze aus § 114 bewiesen.

§ 145. In den voraufgehenden Beweisen nahmen wir für e stets seinen geraden Werth (§ 137—§ 144). Es möge bemerkt werden, dass man auch den ungeraden Werth hätte verwenden können, allein dabei hätte man noch mehr Unterscheidungen einführen müssen. Wer an solchen Untersuchungen Gefallen findet, der wird nicht ohne Nutzen seine Kräfte an

der Entwickelung dieser Fälle üben. Ausserdem hätten dabei die Sätze über die Reste $+2$ und -2 vorausgesetzt werden müssen. Da aber unser Beweis ohne Hülfe jener Theoreme durchgeführt worden ist, so können wir aus ihm eine neue Methode entnehmen, um jene zu beweisen. Dies ist um so weniger zu unterschätzen, als man die Methoden für weniger direct halten kann, welche wir oben zum Beweise des Satzes benutzt haben, dass ± 2 Rest jeder Primzahl von der Form $8n+1$ sei. Von den übrigen, auf die Primzahlen der Formen $8n+3$, $8n+5$, $8n+7$ bezüglichen Sätzen werden wir annehmen, sie seien durch die obigen Methoden bewiesen; nur jenes erste Theorem sei durch Induction gefunden. Und diese Induction wollen wir durch die folgenden Ueberlegungen zur Gewissheit erheben.

Wäre $+2$ nicht von allen Primzahlen der Form $8n+1$ Rest, so werde die kleinste Zahl dieser Form, für die $+2$ Nichtrest ist, gleich a gesetzt, so dass für alle Primzahlen, die kleiner als a sind, das Theorem gilt. Dann nehmen wir irgend eine Primzahl $< \frac{1}{2}a$, für welche a Nichtrest ist (dass es solche giebt, folgt leicht aus § 129). Wir setzen sie $= p$; nach dem Fundamentaltheoreme wird pNa. Daraus ergiebt sich $+2pRa$. Wir setzen daher $e^2 \equiv 2p$ mod. a, derart, dass e ungerade und $< a$ wird. Dann sind zwei Fälle zu unterscheiden.

I. Wenn e nicht durch p theilbar ist, dann sei

$$e^2 = 2p + aq;$$

es wird q positiv, von der Form $8n+7$ oder der Form $8n+3$ je nachdem p von der Form $4n+1$ oder $4n+3$ ist, $< a$ und durch p nicht theilbar. Alle Primfactoren von q mögen in vier Classen verteilt werden: es gebe f von der Form $8n+1$, g von der Form $8n+3$, h von der Form $8n+5$ und k von der Form $8n+7$. Das Product aus den Factoren der ersten Classe sei F, das aus den Factoren der zweiten, dritten, vierten Classe bezw. G, H, K*). Nunmehr wollen wir zuerst den Fall betrachten, dass p von der Form $4n+1$ und q von der Form $8n+7$ ist. Dann erkennt man leicht, es werde $2RF$, $2RK$ und daher pRF, pRK, und endlich FRp, KRp. Ferner wird 2 Nichtrest jedes Factors

*) Giebt es in irgend welcher Classe keinen zugehörigen Factor, so muss man an Stelle des Productes 1 schreiben.

der Form $8n+3$ oder $8n+5$, und also wird auch p Nichtrest jedes solchen Factors; demnach Fundamentaltheorem jeder solche Factor Nichtrest von p. Folglich wird GH Rest für p, wenn $g+h$ gerade wird, dagegen Nichtrest, wenn $g+h$ ungerade wird. Allein $g+h$ kann nicht ungerade sein, denn man erkennt leicht, wenn man alle Fälle aufzählt, dass $FGHK$ d. h. q entweder von der Form $8n+3$ oder $8n+5$ wird, falls $g+h$ ungerade ist, was auch immer die einzelnen f, g, h, k sein mögen; und dies verstösst gegen die Annahme. Daher wird $GHRp$, $FGHKRp$, d. h. qRp und hieraus endlich wegen $aqRp$ gegen die Annahme aRp. — Wenn zweitens p von der Form $4n+3$ ist, dann kann auf ähnliche Art gezeigt werden, dass pRF, also FRp ist, ferner $-pRG$ und also GRp, und endlich, dass $h+k$ gerade und folglich $HKRp$ ist; daraus folgt schliesslich qRp, aRp gegen die Annahme.

II. Wenn e durch p theilbar ist, dann lässt sich der Beweis auf ähnliche Art durchführen, und er kann von Kundigen, für die allein dieser Paragraph geschrieben ist, ohne Schwierigkeit entwickelt werden. Der Kürze halber übergehen wir ihn.



Zweiter Beweis
des Fundamentaltheorems über quadratische Reste[*]

enthalten im fünften Abschnitte § 262 des Werkes

Disquisitiones arithmeticae.

1801.

In dem Falle, dass für eine gegebene nicht quadratische Determinante D nur zwei Charaktere möglich sind, wird nur einem einzigen von ihnen ein eigentlich primitives positives Geschlecht entsprechen und dies muss das Hauptgeschlecht sein, während keiner eigentlich primitiven positiven Form jener Determinante der andere Charakter zukommt. Dies tritt bei den folgenden Werthen der Determinante ein: -1, 2, -2, -4; bei den positiv genommenen Primzahlen von der Form $4n+1$; und bei den negativ genommenen der Form $4n+3$; endlich bei allen positiv genommenen ungeraden Potenzen der Primzahlen von der Form $4n+1$ und bei allen Potenzen der Primzahlen von der Form $4n+3$, welche positiv oder negativ zu nehmen sind, je nachdem die Potenz-Exponenten gerade oder ungerade sind.[*] Aus diesem Princip kann man eine neue Methode schöpfen, um nicht nur das Fundamentaltheorem, sondern auch die übrigen auf die Reste -1, $+2$, -2 bezüglichen Sätze zu beweisen. Sie ist von den oben angewendeten Methoden durchaus verschieden und dürfte ihnen an Eleganz in keiner Weise nachstehen. Wir wollen aber die Fälle, dass die Determinante gleich -4 oder gleich der Potenz einer Primzahl wird, ausschliessen, da sie nichts Neues lehren.

Für die Determinante -1 giebt es also keine positive Form, deren Charakter 3, 4 ist; für die Determinante $+2$ überhaupt keine, deren Charakter 3 *und* 5, 8 ist; für die Determinante -2 kommt keiner positiven Form der Charakter 5 *und* 7, 8 zu; für eine Primzahl-Determinante $+p$, wo p die Gestalt $4n+1$ hat, oder für eine Primzahl-Determinante $-p$, wo p die Gestalt $4n+3$ hat, kommt keiner eigentlich

primitiven (im zweiten Falle zugleich: positiven) Form der Charakter Np zu. Hieraus beweisen wir die in Frage stehenden Theoreme folgendermaassen:

I. Es ist -1 Nichtrest jeder positiven Zahl von der Form $4n+3$. Wäre nämlich -1 Rest einer solchen Zahl A, und setzt man $-1 = B^2 - AC$, dann würde (A, B, C) eine positive Form der Determinante -1 mit dem Charakter 3, 4 (da nämlich $x = 1$, $y = 0$ den Werth A liefert).

II. Es ist -1 Rest jeder Primzahl p von der Form $4n+1$. Denn die Form $(-1, 0, p)$ muss, wie alle eigentlich primitiven Formen der Determinante p den Charakter Rp haben; daher ist $-1\,Rp$.

III. Sowohl $+2$ wie -2 ist Rest jeder Primzahl p der Form $8n+1$. Denn es müssen, je nachdem n ungerade oder gerade ist, entweder die Formen

$$\left(8,\ 1,\ \frac{1-p}{8}\right),\ \left(-8,\ 1,\ \frac{p-1}{8}\right) \quad \text{oder}$$

$$\left(8,\ 3,\ \frac{9-p}{8}\right),\ \left(-8,\ 3,\ \frac{p-9}{8}\right)$$

eigentlich primitive Formen [der Determinante p] werden; sie haben daher den Charakter Rp. Folglich ist $+8\,Rp$ und $-8\,Rp$, und demnach auch $2\,Rp$ und $-2\,Rp$.

IV. Es ist $+2$ Nichtrest jeder Zahl von der Form $8n+3$ und $8n+5$. Wäre nämlich $+2$ Rest einer solchen Zahl A, so gäbe es eine Form (A, B, C) der Determinante $+2$, deren Charakter 3 *und* 5, 8 wäre.

V. Ebenso ist -2 Nichtrest jeder Zahl von der Form $8n+5$ und $8n+7$. Denn sonst gäbe es eine Form (A, B, C) der Determinante -2 mit dem Charakter 5 *und* 7, 8.

VI. Es ist -2 Rest jeder Primzahl p von der Form $8n+3$. Diesen Satz können wir nach zwei verschiedenen Methoden beweisen. Zunächst, da nach IV $+2\,Np$ und nach I. $-1\,Np$, so wird nothwendigerweise $-2\,Rp$. Der zweite Beweis wird aus der Betrachtung der Determinante $2p$ geschöpft. Bei ihr könnten vier Charaktere auftreten, nämlich

Rp; 1 *und* 3, 8. Rp; 5 *und* 7, 8.
Np; 1 *und* 3, 8. Np; 5 *und* 7, 8.

Wenigstens zweien unter diesen entsprechen keine Geschlechter. Nun besitzt $(1, 0, -2p)$ den ersten Charakter und $(-1, 0, 2p)$ den vierten; deshalb sind der zweite und der dritte Charakter zu verwerfen. Da ferner der Charakter der Form $(p, 0, -2)$ hinsichtlich der Zahl 8 durch 1 *und* 3, 8 gegeben ist, so kann ihr Charakter hinsichtlich p nur Rp sein; demnach ist $2Rp$.

VII. Es ist $+2$ Rest jeder Primzahl p von der Form $8n+7$. Dies können wir ebenfalls durch zwei verschiedene Methoden beweisen. Zunächst, da nach I und V $-1Np$ und $-2Np$ ist, so wird $+2Rp$. Zweitens, da entweder

$$\left(8,\ 1,\ \frac{1+p}{8}\right) \quad \text{oder} \quad \left(8,\ 3,\ \frac{9+p}{8}\right)$$

eine eigentlich primitive Form der Determinante $-p$ ist, je nachdem n gerade oder ungerade ist, so hat diese den Charakter Rp; folglich ist $8Rp$ und daher $2Rp$.

VIII. Jede Primzahl p von der Form $4n+1$ ist Nichtrest jeder ungeraden Zahl q, welche selbst Nichtrest von p ist. Denn wenn p ein Rest von q wäre, dann würde es eine eigentlich primitive Form der Determinante p geben, welche den Charakter Np hätte.

IX. Ist irgend eine ungerade Zahl q Nichtrest der Primzahl p von der Form $4n+3$, dann wird $-p$ Nichtrest von q. Denn sonst gäbe es eine positive, eigentlich primitive Form der Determinante $-p$ mit dem Charakter Np.

X. Jede Primzahl p von der Form $4n+1$ ist Rest jeder anderen Primzahl q, welche Rest von p ist. Wenn auch q von der Form $4n+1$ ist, dann folgt dies sofort aus VIII. Ist dagegen q von der Form $4n+3$, dann wird wegen II auch $-q$ Rest von p und also nach IX pRq.

XI. Wenn irgend eine Primzahl q Rest einer anderen Primzahl p von der Form $4n+3$ ist, dann wird $-p$ Rest von q. Ist nämlich q von der Form $4n+1$, dann wird nach VIII pRq, und also nach II $-pRq$. Der Fall, dass auch q von der Form $4n+3$ ist, entzieht sich dieser Methode, doch ist er leicht durch die Betrachtung der Determinante pq zu erledigen. Hier könnten vier Charaktere auftreten, nämlich

$$Rp;\ Rq, \quad Rp;\ Nq, \quad Np;\ Rq, \quad Np;\ Nq.$$

Zweien von ihnen können keine Geschlechter entsprechen; da nun $(1, 0, -pq)$, $(-1, 0, pq)$ Formen mit dem ersten und vierten Charakter sind, so kann zum zweiten und zum dritten Charakter keine eigentlich primitive Form der Determinante pq gehören. Nun ist der Charakter der Form $(q, 0, -p)$ bezüglich der Zahl p nach der Annahme Rp; folglich muss der Charakter derselben Form bezüglich der Zahl q Rq sein; somit ist $-pRq$; w. z. b. w.

Setzt man in den Sätzen VIII und IX q als Primzahl voraus, so geben sie, mit X und XI verbunden, das Fundamentaltheorem.



Neuer [dritter] Beweis eines arithmetischen Satzes [des Fundamentaltheorems]

veröffentlicht in den

Commentationes societatis regiae scientiarum Gottingensis

Vol. XVI; Gottingae 1808.

Werke. Band II: p. 1—8

§ 1. Häufig bieten Fragen der höheren Arithmetik eine merkwürdige Erscheinung, welche in der Analysis bei weitem seltener auftritt und viel dazu beiträgt, den Reiz, der von der höheren Arithmetik ausgeht, zu erhöhen. Während man nämlich bei analytischen Untersuchungen meistens nur dann zu neuen Wahrheiten gelangen kann, wenn man vorher die Principien, auf welche sie sich stützen und welche gewissermaassen den Weg zu ihnen eröffnen, vollständig beherrscht, so springen im Gegensatze dazu in der Arithmetik überaus häufig die elegantesten Sätze mit Hülfe der Induction durch gewissermaassen unerwarteten Glücksfall heraus, während ihre Beweise so tief versteckt liegen und in solche Dunkelheit gehüllt sind, dass sie aller Versuche spotten und selbst den scharfsinnigsten Forschungen sich entziehen. Ferner ist der Zusammenhang zwischen arithmetischen Wahrheiten, die beim ersten Anblick von durchaus verschiedener Natur erscheinen, so gross und so wunderbar, dass man nicht selten bei ganz anderen Forschungen endlich das Glück hat, auf völlig unerwartetem Wege einen Beweis zu finden, den man stark ersehnt und trotz langen Nachdenkens vorher stets vergeblich gesucht hatte. Häufig auch sind solche Wahrheiten der Art, dass man auf mehreren völlig von einander verschiedenen Wegen zu ihnen gelangen kann, und dass die zuerst eingeschlagenen nicht immer die kürzesten sind. Es ist deshalb freudig zu begrüssen, wenn es gelingt eine Wahrheit, die man zunächst lange vergeblich überdacht und dann auch nur auf versteckter liegenden Umwegen hat

beweisen können, endlich auf einfachstem und naturgemässem Wege darzulegen.

§ 2. Unter den Fragen, von welchen wir im vorhergehenden Paragraphen gesprochen haben, nimmt der Satz eine hervorragende Stelle ein, den wir, weil er fast die gesammte Theorie der quadratischen Reste in sich fasst, im vierten Abschnitte der Disquisitiones arithmeticae durch den Namen »Fundamentaltheorem« ausgezeichnet haben. Als erster Entdecker dieses überaus eleganten Satzes muss *Legendre* angesehen werden, nachdem lange zuvor die hochbedeutenden Geometer *Euler* und *Lagrange* schon mehrere besondere Fälle dieses Satzes durch Induction entdeckt hatten*). Ich verweile hier nicht bei der Aufzählung der Versuche dieser Männer, den Beweis zu liefern; wem es Vergnügen bereitet, der möge das oben erwähnte Werk nachlesen. Es möge nur zur Bestätigung des im vorigen Paragraphen Behaupteten gestattet sein, auf meine eigenen Versuche Bezug zu nehmen. Auf den Satz selbst kam ich völlig selbständig im Jahre 1795, zu einer Zeit, da ich mich in völliger Unkenntniss über Alles befand, was in der höheren Arithmetik bereits erreicht worden war, und zugleich nicht die mindesten litterarischen Hülfsmittel besass. Ein ganzes Jahr lang quälte mich dieser Satz und entzog sich den angestrengtesten Bemühungen, bis ich endlich den im vierten Abschnitte jenes Werkes gegebenen Beweis erlangte. Später stiess ich dann auf drei andere, welche sich auf vollkommen verschiedenen Principien aufbauten; den einen derselben habe ich schon im fünften Abschnitte behandelt; die übrigen, welche jenem an Eleganz in keiner Weise nachstehen, habe ich mir für eine andere Gelegenheit zur Veröffentlichung aufgespart. Wiewohl aber alle diese Beweise jeder Anforderung an Strenge genügen, so sind sie doch aus gar zu weit abseits gelegenen Quellen hergeleitet, ausgenommen vielleicht der erste, der dafür wieder mit schwierigeren Schlussfolgerungen vorgeht und mit weitläufigen Operationen belastet ist. Ich stehe nicht an, auszusprechen, dass bisher ein naturgemässer Beweis nicht beigebracht worden ist. Jetzt mögen Sachverständige darüber urtheilen, ob der auf den folgenden Seiten behandelte, den wir neulich zu entdecken so glücklich waren, mit dieser Bezeichnung belegt zu werden verdient.

*) [Vgl. Anmerkung 1.

§ 3. Lehrsatz. Es möge p eine positive Primzahl und k eine durch p nicht theilbare beliebige Zahl sein; ferner

A der Complex der Zahlen $1.2.3. \ldots \frac{1}{2}(p-1)$

B der Complex der Zahlen $\frac{1}{2}(p+1). \frac{1}{2}(p+3).$
$\frac{1}{2}(p+5). \ldots p-1.$

Wir bestimmen die kleinsten positiven Reste modulo p der Producte aus k in die einzelnen Zahlen A; diese werden offenbar sämmtlich unter einander verschieden sein und theils zu A theils zu B gehören. Setzt man nun voraus, dass μ dieser Reste zu B gehören, dann wird k quadratischer Rest oder Nichtrest von p, je nachdem μ gerade oder ungerade ist.

Beweis. Die zu A gehörigen Reste bezeichnen wir mit $a, a', a'' \ldots$ und die übrigen, die zu B gehören, mit $b, b', b'' \ldots$; dann ist es klar, dass die Complemente dieser letzten, $p-b$, $p-b'$, $p-b''$, ... sämmtlich von den Zahlen $a, a', a'', \ldots$ verschieden sind, und dass sie mit diesen zusammengenommen den Complex A geben. Wir haben folglich

$$1.2.3. \ldots. \tfrac{1}{2}(p-1) = aa'a'' \ldots (p-b)(p-b')(p-b'') \ldots$$

Das zweite Product wird offenbar mod. p

$$\equiv (-1)^{\mu} aa'a'' \ldots bb'b'' \ldots \equiv (-1)^{\mu} k.2k.3k \ldots \tfrac{1}{2}(p-1)k$$
$$\equiv (-1)^{\mu} k^{\frac{1}{2}(p-1)} 1.2.3 \ldots \tfrac{1}{2}(p-1).$$

Folglich wird

$$1 \equiv (-1)^{\mu} k^{\frac{1}{2}(p-1)},$$

d. h. $k^{\frac{1}{2}(p-1)} \equiv \pm 1$, je nachdem μ gerade oder ungerade ist. Hieraus ergiebt sich sofort unser Lehrsatz. (Vgl. S. 11.)

§ 4. Man kann die folgenden Schlüsse durch Einführung gewisser geeigneter Bezeichnungen sehr abkürzen. Das Symbol (k, p) soll uns die Menge derjenigen Producte unter

$$1.k,\ 2k,\ 3k, \ldots \tfrac{1}{2}(p-1)k$$

angeben, deren kleinste positive Reste modulo p grösser sind als $\frac{p}{2}$. Wenn ferner x irgend eine Grösse bezeichnet, welche nicht ganz ist, dann drücken wir durch das Zeichen $[x]$ die nächst kleinere ganze Zahl aus, so dass $x-[x]$ stets eine

positive, zwischen den Grenzen 0 und 1 gelegene Grösse wird. Mit leichter Mühe kann man die folgenden Relationen entwickeln.

I. $[x] + [-x] = -1$.

II. $[x] + h = [x + h]$, falls h ganz ist.

III. $[x] + [h - x] = h - 1$.

IV. Wenn $x - [x]$ ein Bruch ist, der $< \frac{1}{2}$ bleibt, dann wird $[2x] - 2[x] = 0$, wenn dagegen $x - [x] > \frac{1}{2}$ wird, dann ist $[2x] - 2[x] = 1$.

V. Liegt daher der kleinste positive Rest von k modulo p unterhalb $\frac{1}{2}p$, dann wird $\left[\frac{2k}{p}\right] - 2\left[\frac{k}{p}\right] = 0$; liegt er aber oberhalb $\frac{1}{2}p$, dann wird $\left[\frac{2k}{p}\right] - 2\left[\frac{k}{p}\right] = 1$.

VI. Hieraus folgt sofort

$$(k, p) = \left[\frac{2k}{p}\right] + \left[\frac{4k}{p}\right] + \left[\frac{6k}{p}\right] + \cdots + \left[\frac{(p-1)k}{p}\right]$$
$$- 2\left[\frac{k}{p}\right] - 2\left[\frac{2k}{p}\right] - 2\left[\frac{3k}{p}\right] - \cdots - 2\left[\frac{\frac{1}{2}(p-1)k}{p}\right].$$

VII. Aus VI und I leitet man ohne Mühe

$$(k, p) + (-k, p) = \tfrac{1}{2}(p - 1)$$

her. Hieraus folgt, dass $-k$ hinsichtlich des quadratischen Rest- oder Nichtrestcharakters die gleiche oder die entgegengesetzte Beziehung zu p hat wie k, je nachdem p von der Form $4n + 1$ oder von der Form $4n + 3$ ist. Im ersten Falle ist offenbar -1 Rest und im zweiten Nichtrest von p.

VIII. Die in VI hergeleitete Formel transformiren wir folgendermaassen. Nach III wird

$$\left[\frac{(p-1)k}{p}\right] = k - 1 - \left[\frac{k}{p}\right], \quad \left[\frac{(p-3)k}{p}\right] = k - 1 - \left[\frac{3k}{p}\right],$$
$$\left[\frac{(p-5)k}{p}\right] = k - 1 - \left[\frac{5k}{p}\right], \cdots$$

Wenn man diese Substitutionen auf die $\frac{p \mp 1}{4}$ letzten Glieder der oberen Reihe jenes Ausdruckes anwendet, dann erhält man [10],

erstens, falls p von der Form $4n+1$ ist,

$$(k,p) = \tfrac{1}{4}(k-1)(p-1) - 2\left\{\left[\frac{k}{p}\right]+\left[\frac{3k}{p}\right]+\cdots+\left[\frac{\frac{1}{2}(p-3)k}{p}\right]\right\}$$
$$-\left\{\left[\frac{k}{p}\right]+\left[\frac{2k}{p}\right]+\cdots+\left[\frac{\frac{1}{2}(p-1)k}{p}\right]\right\};$$

zweitens, falls p von der Form $4n+3$ ist,

$$(k,p) = \tfrac{1}{4}(k-1)(p+1) - 2\left\{\left[\frac{k}{p}\right]+\left[\frac{3k}{p}\right]+\cdots+\left[\frac{\frac{1}{2}(p-1)k}{p}\right]\right\}$$
$$-\left\{\left[\frac{k}{p}\right]+\left[\frac{2k}{p}\right]+\cdots+\left[\frac{\frac{1}{2}(p-1)k}{p}\right]\right\}.$$

IX. In dem besonderen Falle $k=2$ folgt aus den eben aufgestellten Formeln (da alle Summanden in den geschweiften Klammern Null werden, weil ihre Argumente echte Brüche sind), $(2,p) = \frac{1}{4}(p \mp 1)$, indem man das obere oder das untere Zeichen nimmt, je nachdem p von der Form $4n+1$ oder $4n+3$ ist. Es wird also $(2,p)$ gerade und folglich $2Rp$, falls p von der Form $8n+1$ oder $8n+7$ ist; dagegen wird $(2,p)$ ungerade und folglich $2Np$, falls p von der Form $8n+3$ oder $8n+5$ ist.

§ 5. **Lehrsatz.** Es sei x eine positive, nicht ganzzahlige Grösse, unter deren Vielfachen $x, 2x, 3x, \ldots$ bis zu nx keine ganze Zahl vorkommt; wird $[nx] = h$ gesetzt, so schliesst man leicht, dass auch unter den Vielfachen der reciproken Grösse $\frac{1}{x}, \frac{2}{x}, \frac{3}{x}, \ldots$ bis zu $\frac{h}{x}$ keine ganze Zahl sich findet. Dann behaupte ich, dass man hat

$$\left.\begin{array}{l} [x]+[2x]+[3x]+\cdots+[nx] \\ +\left[\frac{1}{x}\right]+\left[\frac{2}{x}\right]+\left[\frac{3}{x}\right]+\cdots+\left[\frac{h}{x}\right] \end{array}\right\} = nh.$$

Beweis. In der Reihe $[x]+[2x]+[3x]+\cdots+[nx]$, die wir $= \Omega$ setzen wollen, werden alle Glieder vom ersten bis zum $\left[\frac{1}{x}\right]^{\text{ten}}$ incl. offenbar $= 0$; die darauf folgenden bis

zum $\left[\frac{2}{x}\right]^{\text{ten}}$ insgesammt $= 1$; die folgenden bis zum $\left[\frac{3}{x}\right]^{\text{ten}}$ alle $= 2$ und so fort. Daher wird

$$\Omega = 0.\left[\frac{1}{x}\right] + 1.\left\{\left[\frac{2}{x}\right] - \left[\frac{1}{x}\right]\right\} + 2.\left\{\left[\frac{3}{x}\right] - \left[\frac{2}{x}\right]\right\}$$

$$+ 3.\left\{\left[\frac{4}{x}\right] - \left[\frac{3}{x}\right]\right\} + \cdots + h - 1\left\{\left[\frac{h}{x}\right] - \left[\frac{h-1}{x}\right]\right\}$$

$$+ h\left\{n - \left[\frac{h}{x}\right]\right\}$$

$$= hn - \left[\frac{1}{x}\right] - \left[\frac{2}{x}\right] - \left[\frac{3}{x}\right] - \cdots - \left[\frac{h}{x}\right], \text{ w. z. b. w.}$$

§ 6. Lehrsatz. Bezeichnen k, p irgend welche positive, ungerade, zu einander theilerfremde Zahlen, dann wird

$$\left.\begin{matrix}\left[\frac{k}{p}\right] + \left[\frac{2k}{p}\right] + \left[\frac{3k}{p}\right] + \cdots + \left[\frac{\frac{1}{2}(p-1)k}{p}\right] \\ + \left[\frac{p}{k}\right] + \left[\frac{2p}{k}\right] + \left[\frac{3p}{k}\right] + \cdots + \left[\frac{\frac{1}{2}(k-1)p}{k}\right]\end{matrix}\right\} = \tfrac{1}{4}(k-1)(p-1).$$

Beweis. Setzt man, was angeht, $k < p$ voraus, dann wird $\frac{\frac{1}{2}(p-1)k}{p} < \frac{1}{2}k$ aber $> \frac{1}{2}(k-1)$ und also

$$\left[\frac{\frac{1}{2}(p-1)k}{p}\right] = \tfrac{1}{2}(k-1).$$

Hiernach ist klar, dass der eben ausgesprochene Lehrsatz aus dem vorhergehenden sogleich folgt, wenn man dort $\frac{k}{p} = x$, $\frac{1}{2}(p-1) = n$ und also $\frac{1}{2}(k-1) = h$ setzt.

Man kann übrigens auf ähnliche Weise zeigen, dass, wenn k eine gerade zu p theilerfremde Zahl ist, dann

$$\left.\begin{matrix}\left[\frac{k}{p}\right] + \left[\frac{2k}{p}\right] + \left[\frac{3k}{p}\right] + \cdots + \left[\frac{\frac{1}{2}(p-1)k}{p}\right] \\ + \left[\frac{p}{k}\right] + \left[\frac{2p}{k}\right] + \left[\frac{3p}{k}\right] + \cdots + \left[\frac{\frac{1}{2}kp}{k}\right]\end{matrix}\right\} = \tfrac{1}{4}k(p-1)$$

wird. Jedoch verweilen wir nicht bei diesem Satze, da er für unseren Zweck nicht nothwendig ist.

§ 7. Jetzt fliesst aus der Zusammenstellung des letzten Lehrsatzes mit dem Satze VIII., § 4 sofort das Fundamentaltheorem. Bezeichnen nämlich k, p irgend welche positiven ungleichen [ungeraden] Primzahlen, und setzt man

$$(k, p) + \left[\frac{k}{p}\right] + \left[\frac{2k}{p}\right] + \left[\frac{3k}{p}\right] + \cdots + \left[\frac{\frac{1}{2}(p-1)k}{p}\right] = L,$$

$$(p, k) + \left[\frac{p}{k}\right] + \left[\frac{2p}{k}\right] + \left[\frac{3p}{k}\right] + \cdots + \left[\frac{\frac{1}{2}(k-1)p}{k}\right] = M,$$

so folgt aus § 4, VIII., dass L und M stets gerade Zahlen werden. Aus dem Lehrsatze des § 6 folgt

$$L + M = (k, p) + (p, k) + \tfrac{1}{4}(k-1)(p-1).$$

So oft also $\frac{1}{4}(k-1)(p-1)$ gerade wird, d. h. wenn k, p beide oder wenigstens eine dieser Zahlen von der Form $4n+1$ ist, müssen (k, p) und (p, k) entweder beide gerade, oder beide ungerade sein. So oft dagegen $\frac{1}{4}(k-1)(p-1)$ ungerade wird, d. h. wenn k, p beide von der Form $4n+3$ sind, dann muss nothwendigerweise von den beiden Zahlen (k, p), (p, k) die eine gerade und die andere ungerade werden. Im ersten Falle sind die Relationen von k zu p und von p zu k (hinsichtlich des Charakters als Rest oder Nichtrest der einen in Beziehung auf die andere) mit einander identisch; im zweiten Falle sind sie einander entgegengesetzt.



Vierter Beweis des Fundamentaltheorems

enthalten in der Abhandlung:

Summirung einiger merkwürdigen Reihen.[11]

Veröffentlicht in den

Commentationes societatis regiae scientiarum Gottingensis recentiores.

Vol. I; Gottingae 1811.

(Werke, Band II; p. 9—45.)

§ 1. Unter den bedeutsameren Wahrheiten, zu welchen die Theorie der Kreistheilung den Zugang eröffnet hat, gebührt sicher nicht die letzte Stelle der in den (Disquisitiones arithmeticae) § 356 gelieferten Summation, und zwar nicht allein wegen ihrer ganz besonderen Eleganz und ihrer wunderbaren Fruchtbarkeit, die in einer späteren Abhandlung ausführlich darzulegen Gelegenheit sein wird, sondern auch deswegen, weil ein strenger und vollständiger Beweis auf ganz ungewöhnliche Schwierigkeiten stösst. Diese liessen sich um so weniger erwarten, als sie nicht eigentlich dem Theoreme selbst anhaften, sondern vielmehr einer gewissen Eingrenzung des Lehrsatzes: vernachlässigen wir diese, dann liegt der Beweis sofort auf der Hand: er fliesst auf die einfachste Art aus der in jenem Werke dargelegten Theorie. Der Lehrsatz ist dort in der folgenden Form auseinander gesetzt. Bedeutet n eine Primzahl: bezeichnet man alle quadratischen Reste von n, die zwischen 1 und $(n-1)$ incl. liegen, unbestimmt durch a; alle zwischen denselben Grenzen liegenden Nichtreste durch b; endlich den Bogen $\frac{360^0}{n}$ durch ω, und durch k eine beliebige aber bestimmte, durch n nicht theilbare Zahl, so wird

I. für einen Werth von n, der die Form $4m+1$ hat,

$$\Sigma \cos a k \omega = -\tfrac{1}{2} \pm \tfrac{1}{2} \sqrt{n},$$
$$\Sigma \cos b k \omega = -\tfrac{1}{2} \mp \tfrac{1}{2} \sqrt{n}, \quad \text{und also}$$
$$\Sigma \cos a k \omega - \Sigma \cos b k \omega = \pm \sqrt{n},$$
$$\Sigma \sin a k \omega = 0,$$
$$\Sigma \sin b k \omega = 0;$$

II. für einen Werth von n, der die Form $4m+3$ hat,

$$\Sigma \cos a k \omega = -\tfrac{1}{2},$$
$$\Sigma \cos b k \omega = -\tfrac{1}{2},$$
$$\Sigma \sin a k \omega = \pm \tfrac{1}{2} \sqrt{n},$$
$$\Sigma \sin b k \omega = \mp \tfrac{1}{2} \sqrt{n},$$
$$\Sigma \sin a k \omega - \Sigma \sin b k \omega = \pm \sqrt{n}.$$

Diese Summationen sind a. a. O. in aller Strenge bewiesen: so dass nur die Schwierigkeit zurückbleibt, das Zeichen zu bestimmen, welches der Wurzelgrösse vorgesetzt werden muss. Ohne jede Mühe lässt sich zeigen, dass dieses Zeichen nur in so fern von k abhänge, als stets für alle Werthe von k, welche quadratische Reste von n sind, ein bestimmtes Zeichen; und für alle Werthe von k, welche quadratische Nichtreste von n sind, das jenem entgegengesetzte Zeichen gilt. Daher dreht sich die ganze Aufgabe um den Werth $k=1$; und es ist klar, dass, sobald man nur das für diesen Werth geltende Zeichen gefunden hat, für alle übrigen Werthe von k die Zeichen sofort bekannt sein werden. Diese Aufgabe scheint beim ersten Anblicke zu den leichteren zu gehören; gleichwohl stiessen wir dabei auf unvorhergesehene Schwierigkeiten, und die Methode, welche uns bis dahin ohne Hindernisse geführt hatte, lässt uns weiterhin vollkommen im Stiche*).

§ 4. In allen berechneten Beispielen erhält die Wurzelgrösse das positive Vorzeichen: daraus entspringt eine starke Wahrscheinlichkeit, dass dies sich überhaupt so verhalten werde. Aber der Beweis dieser Thatsache lässt sich aus den a. a. O. gegebenen Grundsätzen nicht herleiten und ist mit vollstem Rechte als viel tiefer liegend anzusehen. Der Zweck

---

*) [Die §§ 2 und 3, in denen nach einigen allgemeinen Bemerkungen numerische Beispiele durchgeführt sind, habe ich der Kürze halber unterdrückt.]

dieser Abhandlung ist, einen strengen Beweis dieses höchst eleganten Satzes bekannt zu geben; wir haben einen solchen früher mehrere Jahre hindurch auf verschiedene Arten, aber stets vergeblich, zu führen gesucht und ihn endlich durch eigenthümliche und ziemlich versteckt liegende Betrachtungen glücklich zu Stande gebracht. Zugleich werden wir das Theorem selbst ohne Verminderung, ja sogar mit Erhöhung seiner Eleganz in bei weitem grösserer Allgemeinheit darlegen. Schliesslich werden wir den merkwürdigen, sehr engen Zusammenhang zwischen dieser Summation und einem anderen überaus wichtigen arithmetischen Theoreme zeigen. Wir hoffen, dass diese Untersuchungen nicht nur um ihrer selbst willen den Mathematikern willkommen sein werden, sondern dass sich auch die Methoden ihrer Beachtung werth zeigen, durch welche dies Alles erlangt werden konnte und die auch bei anderen Gelegenheiten sich nützlich erweisen dürften.

§ 5. Unser Beweis gründet sich auf die Betrachtung einer merkwürdigen Art von Reihen, deren Glieder von Ausdrücken der Form

$$\frac{(1-x^m)(1-x^{m-1})(1-x^{m-2})\ldots\ldots(1-x^{m-\mu+1})}{(1-x)(1-x^2)(1-x^3)\ldots\ldots(1-x^\mu)}$$

abhängen. Der Kürze halber bezeichnen wir einen solchen Bruch durch (m, μ) und wollen zunächst einige allgemeine Bemerkungen über derartige Functionen voranschicken.

I. Falls m eine ganze Zahl und kleiner als μ ist, verschwindet offenbar die Function (m, μ), da sie im Zähler den Factor $1-x^0$ enthält. Für $m=\mu$ werden die Factoren des Zählers in umgekehrter Reihenfolge identisch mit denen des Nenners, so dass $(\mu, \mu)=1$ ist; endlich hat man für den Fall, dass m eine ganze positive Zahl und grösser als μ ist, die Formeln

$$(\mu+1, \mu)=\frac{1-x^{\mu+1}}{1-x}=(\mu+1, 1),$$

$$(\mu+2, \mu)=\frac{(1-x^{\mu+2})(1-x^{\mu+1})}{(1-x)(1-x^2)}=(\mu+2, 2),$$

$$(\mu+3, \mu)=\frac{(1-x^{\mu+3})(1-x^{\mu+2})(1-x^{\mu+1})}{(1-x)(1-x^2)(1-x^3)}=(\mu+3, 3), \ldots$$

und allgemein

$$(m, \mu)=(m, m-\mu).$$

II. Ferner erkennt man leicht, dass allgemein

$$(m, \mu + 1) = (m - 1, \mu + 1) + x^{m - \mu - 1}(m - 1, \mu)$$

wird, so dass man also auch

$$(m - 1, \mu + 1) = (m - 2, \mu + 1) + x^{m - \mu - 2}(m - 2, \mu),$$
$$(m - 2, \mu + 1) = (m - 3, \mu + 1) + x^{m - \mu - 3}(m - 3, \mu),$$
$$(m - 3, \mu + 1) = (m - 4, \mu + 1) + x^{m - \mu - 4}(m - 4, \mu) \ldots$$

setzen darf. Diese Reihe kann bis zu

$$(\mu + 2, \mu + 1) = (\mu + 1, \mu + 1) + x(\mu + 1, \mu)$$
$$= (\mu, \mu) + x(\mu + 1, \mu)$$

fortgesetzt werden. Wenn m eine positive ganze Zahl und grösser als $\mu + 1$ ist, dann wird demnach

$$(m, \mu + 1) = (\mu, \mu) + x(\mu + 1, \mu) + x^2(\mu + 2, \mu)$$
$$+ x^3(\mu + 3, \mu) + \ldots + x^{m - \mu - 1}(m - 1, \mu).$$

Hieraus ersieht man, dass, wenn für irgend einen bestimmten Werth von μ jede Function (m, μ) ganz ist bei positivem ganzen m, dann auch jede Function $(m, \mu + 1)$ ganz wird. Da nun unsere Annahme für $\mu = 1$ statt hat, so gilt sie auch für $\mu = 2$, deswegen dann auch für $\mu = 3$, u. s. f., d. h. es wird allgemein für jeden beliebigen ganzen positiven Werth von m die Function (m, μ) ganz, d. h. das Product

$$(1 - x^m)(1 - x^{m-1})(1 - x^{m-2}) \ldots (1 - x^{m - \mu + 1})$$

wird theilbar durch

$$(1 - x)(1 - x^2)(1 - x^3) \ldots (1 - x^\mu).$$

§ 6. Wir betrachten nun zwei Reihen, die uns beide zum Ziele führen können. Die erste Reihe lautet

$$1 - \frac{1 - x^m}{1 - x} + \frac{(1 - x^m)(1 - x^{m-1})}{(1 - x)(1 - x^2)}$$
$$- \frac{(1 - x^m)(1 - x^{m-1})(1 - x^{m-2})}{(1 - x)(1 - x^2)(1 - x^3)} + \ldots$$

oder

$$1 - (m, 1) + (m, 2) - (m, 3) + (m, 4) - \cdots;$$

wir bezeichnen sie der Kürze halber mit $f(x, m)$. Zunächst ist es sofort ersichtlich, dass diese Reihe, falls m eine ganze

positive Zahl ist, nach dem $(m+1)^{\text{ten}}$ Gliede (welches $= \pm 1$ wird), abbreche, so dass in diesem Falle die Summe eine endliche ganze Function von x wird. Ferner zeigt § 5, II., dass für jeden Werth von m allgemein

$$\begin{aligned} 1 &= 1 \\ -(m,1) &= -(m-1,1) - x^{m-1}, \\ +(m,2) &= +(m-1,2) + x^{m-2}(m-1,1), \\ -(m,3) &= -(m-1,3) - x^{m-3}(m-1,2), \ldots \end{aligned}$$

gilt, und daher wird

$$f(x,m) = 1 - x^{m-1} - (1-x^{m-2})(m-1,1) + (1-x^{m-3})(m-1,2) - (1-x^{m-4})(m-1,3) + \cdots$$

Offenbar ist aber

$$\begin{aligned} (1-x^{m-2})(m-1,1) &= (1-x^{m-1})(m-2,1) \\ (1-x^{m-3})(m-1,2) &= (1-x^{m-1})(m-2,2) \\ (1-x^{m-4})(m-1,3) &= (1-x^{m-1})(m-2,3), \ldots \end{aligned}$$

und daraus erschliessen wir die Gleichung

$$(1) \qquad f(x,m) = (1-x^{m-1}) f(x, m-2).$$

§ 7. Da für $m=0$ sich $f(x,m)=1$ ergiebt, so wird nach der soeben gefundenen Formel

$$\begin{aligned} f(x,2) &= 1-x, \\ f(x,4) &= (1-x)(1-x^3), \\ f(x,6) &= (1-x)(1-x^3)(1-x^5), \\ f(x,8) &= (1-x)(1-x^3)(1-x^5)(1-x^7), \ldots \end{aligned}$$

oder allgemein für irgend welchen geraden Werth von m

$$(2) \qquad f(x,m) = (1-x)(1-x^3)(1-x^5)\ldots(1-x^{m-1}).$$

Für $m=1$ wird dagegen $f(x,m)=0$, und daher ist auch

$$\begin{aligned} f(x,3) &= 0, \\ f(x,5) &= 0, \\ f(x,7) &= 0, \ldots \end{aligned}$$

oder allgemein für irgend welchen ungeraden Werth von m

$$f(x,m) = 0.$$

Uebrigens hätten wir diese letzte Summation auch daraus ableiten können, dass in der Reihe

$$1 - (m,1) + (m,2) - (m,3) + \cdots + (m, m-1) - (m,m)$$

das letzte Glied sich gegen das erste hebt, das vorletzte gegen das zweite, u. s. f.

§ 8. Für unseren Zweck genügt zwar der Fall, dass m eine positive ungerade Zahl ist, aber wegen der Eigenart der Verhältnisse wird es nicht unangebracht sein, auch Einiges über den Fall hinzuzufügen, in welchem m gebrochen oder negativ ist. Offenbar wird dann unsere Reihe nicht mehr abbrechen, sondern ins Unendliche fortgehen; da man ausserdem leicht einsieht, dass sie divergent wird, wenn man dem x einen Werth < 1 giebt, so muss man die Summation auf Werthe von x, die grösser als 1 sind, beschränken.

Nach der Formel (1) aus § 6 haben wir

$$f(x, -2) = \frac{1}{1 - \frac{1}{x}},$$

$$f(x, -4) = \frac{1}{1 - \frac{1}{x}} \cdot \frac{1}{1 - \frac{1}{x^3}},$$

$$f(x, -6) = \frac{1}{1 - \frac{1}{x}} \cdot \frac{1}{1 - \frac{1}{x^3}} \cdot \frac{1}{1 - \frac{1}{x^5}} \cdots,$$

so dass der Werth der Function $f(x, m)$ auch für einen negativen, ganzen, geraden Werth von m in endlicher Form darstellbar ist. Für die übrigen Werthe von m dagegen wandeln wir die Function $f(x, m)$ auf folgende Art in ein unendliches Product um.

Wächst m ins negativ Unendliche, dann geht $f(x, m)$ über in

$$1 + \frac{1}{x-1} + \frac{1}{x-1} \cdot \frac{1}{x^2-1} + \frac{1}{x-1} \cdot \frac{1}{x^2-1} \cdot \frac{1}{x^3-1} + \cdots$$

Diese Reihe ist daher dem unendlichen Producte

$$\frac{1}{1 - \frac{1}{x}} \cdot \frac{1}{1 - \frac{1}{x^3}} \cdot \frac{1}{1 - \frac{1}{x^5}} \cdot \frac{1}{1 - \frac{1}{x^7}} \cdots$$

gleich. Weil ferner allgemein (nach § 6, (1))

$$f(x, m) = f(x, m-2\lambda) \cdot (1-x^{m-1})(1-x^{m-3})(1-x^{m-5}) \ldots (1-x^{m-2\lambda+1})$$

gilt, so wird

$$f(x, m) = f(x, -\infty) \cdot (1-x^{m-1})(1-x^{m-3})(1-x^{m-5}) \ldots$$
$$= \frac{1-x^{m-1}}{1-x^{-1}} \cdot \frac{1-x^{m-3}}{1-x^{-3}} \cdot \frac{1-x^{m-5}}{1-x^{-5}} \cdot \frac{1-x^{m-7}}{1-x^{-7}} \cdot \ldots;$$

es ist offenbar, dass die Factoren schliesslich beständig mehr und mehr zur Einheit hin convergiren.

Besondere Aufmerksamkeit verdient der Fall $m = -1$; hier wird

$$f(x, -1) = 1 + x^{-1} + x^{-3} + x^{-6} + x^{-10} + \cdots;$$

und dies wird sonach gleich dem unendlichen Producte

$$\frac{1-x^{-2}}{1-x^{-1}} \cdot \frac{1-x^{-4}}{1-x^{-3}} \cdot \frac{1-x^{-6}}{1-x^{-5}} \ldots$$

Schreibt man nun x statt x^{-1}, so entsteht

$$1 + x^1 + x^3 + x^6 + \cdots = \frac{1-x^2}{1-x} \cdot \frac{1-x^4}{1-x^3} \cdot \frac{1-x^6}{1-x^5} \cdot \frac{1-x^8}{1-x^7} \ldots$$

Diese Gleichung zwischen zwei merkwürdigen Ausdrücken ist recht beachtenswerth; ich werde bei anderer Gelegenheit auf sie zurückkommen.

§ 9. An zweiter Stelle ziehen wir die Reihe

$$1 + x^{\frac{1}{2}} \frac{1-x^m}{1-x} + x \frac{(1-x^m)(1-x^{m-1})}{(1-x)(1-x^2)}$$
$$+ x^{\frac{3}{2}} \frac{(1-x^m)(1-x^{m-1})(1-x^{m-2})}{(1-x)(1-x^2)(1-x^3)} + \cdots$$

oder

$$1 + x^{\frac{1}{2}}(m, 1) + x(m, 2) + x^{\frac{3}{2}}(m, 3) + x^2(m, 4) + \cdots,$$

die wir durch $F(x, m)$ bezeichnen wollen, in Betracht. Wir werden diese Untersuchung auf den Fall beschränken, dass m eine ganze positive Zahl ist, so dass auch diese Reihe beständig mit dem $(m+1)^{\text{ten}}$ Gliede, welches $= x^{\frac{1}{2}m}(m, m)$ ist, abbrechen wird. Da

$$(m, m) = 1, \quad (m, m-1) = (m, 1), \quad (m, m-2) = (m, 2), \ldots$$

wird, so kann unsere Reihe auch so dargestellt werden:

$$F(x, m) = x^{\frac{1}{2}m} + x^{\frac{1}{2}(m-1)}(m, 1) + x^{\frac{1}{2}(m-2)}(m, 2) + x^{\frac{1}{2}(m-3)}(m, 3) + \cdots$$

Demnach wird

$$(1 + x^{\frac{1}{2}m+\frac{1}{2}}) . F(x, m) = 1 + x^{\frac{1}{2}}(m, 1) + x(m, 2) + x^{\frac{3}{2}}(m, 3) + \cdots$$
$$+ x^{\frac{1}{2}} . x^m + x . x^{m-1}(m, 1) + x^{\frac{3}{2}} . x^{m-2}(m, 2) + \cdots$$

Nun hat man (§ 5, II)

$$(m, 1) + x^m = (m + 1, 1),$$
$$(m, 2) + x^{m-1}(m, 1) = (m + 1, 2),$$
$$(m, 3) + x^{m-2}(m, 2) = (m + 1, 3), \ldots,$$

und daraus entspringt

$$(3) \qquad (1 + x^{\frac{1}{2}m+\frac{1}{2}}) F(x, m) = F(x, m + 1).$$

Es ist aber $F(x, 0) = 1$; demgemäss wird

$$F(x, 1) = 1 + x^{\frac{1}{2}}$$
$$F(x, 2) = (1 + x^{\frac{1}{2}})(1 + x)$$
$$F(x, 3) = (1 + x^{\frac{1}{2}})(1 + x)(1 + x^{\frac{3}{2}}), \ldots$$

oder allgemein

$$(4) \qquad F(x, m) = (1 + x^{\frac{1}{2}})(1 + x)(1 + x^{\frac{3}{2}}) \ldots (1 + x^{\frac{1}{2}m}).$$

§ 10. Nach Erledigung dieser vorbereitenden Untersuchungen treten wir unserer Aufgabe näher. Da für einen Primzahlwerth n die Quadrate 1, 4, 9, ... $(\frac{1}{2}(n-1))^2$ sämmtlich unter einander incongruent modulo n sind, so ist es klar, dass ihre kleinsten Reste nach diesem Modul mit den Zahlen a identisch sein müssen; demnach hat man

$$\Sigma \cos ak\omega = \cos k\omega + \cos 4k\omega + \cos 9k\omega + \cdots + \cos(\tfrac{1}{2}(n-1))^2 k\omega,$$
$$\Sigma \sin ak\omega = \sin k\omega + \sin 4k\omega + \sin 9k\omega + \cdots + \sin(\tfrac{1}{2}(n-1))^2 k\omega.$$

Da ferner dieselben Quadrate 1, 4, 9, ..., $(\frac{1}{2}(n-1))^2$ in umgekehrter Ordnung den folgenden $(\frac{1}{2}(n+1))^2$, $(\frac{1}{2}(n+3))^2$, $(\frac{1}{2}(n+5))^2$, ... $(n-1)^2$ congruent sind, so sind auch

$$\Sigma \cos ak\omega = \cos(\tfrac{1}{2}(n+1))^2 k\omega + \cos(\tfrac{1}{2}(n+3))^2 k\omega + \cdots + \cos(n-1)^2 k\omega,$$
$$\Sigma \sin ak\omega = \sin(\tfrac{1}{2}(n+1))^2 k\omega + \sin(\tfrac{1}{2}(n+3))^2 k\omega + \cdots + \sin(n-1)^2 k\omega.$$

Setzt man daher

$$T = 1 + \cos k\omega + \cos 4k\omega + \cos 9k\omega + \cdots + \cos (n-1)^2 k\omega,$$
$$U = \sin k\omega + \sin 4k\omega + \sin 9k\omega + \cdots + \sin (n-1)^2 k\omega,$$

so wird
$$1 + 2\Sigma \cos a k\omega = T,$$
$$2\Sigma \sin a k\omega = U.$$

Hieraus erhellt, dass die in § 1 vorgelegten Summationen von denjenigen der Reihen T und U abhängen. Wir lassen deshalb jene bei Seite, richten unsere Untersuchung auf diese und werden sie in solcher Allgemeinheit durchführen, dass wir sie nicht allein für Primzahlwerthe von n, sondern auch für alle zusammengesetzten Werthe erledigen. Dagegen nehmen wir k stets als zu n theilerfremd an: auf diesen Fall lässt sich nämlich ohne Mühe derjenige zurückführen, in welchem k und n einen gemeinsamen Theiler besitzen.

§ 11. Wir wollen die imaginäre Grösse $\sqrt{-1}$ mit i bezeichnen und setzen

$$\cos k\omega + i \sin k\omega = r;$$

dann wird $r^n = 1$, d. h. r eine Wurzel der Gleichung

$$x^n - 1 = 0.$$

Man erkennt leicht, dass alle Zahlen $k, 2k, 3k, \ldots (n-1)k$ durch n nicht theilbar und unter sich incongruent modulo n sein werden. Folglich werden die Potenzen

$$1, r, r^2, r^3, \ldots r^{n-1}$$

sämmtlich ungleich. Da aber eine jede der Gleichung $x^n - 1 = 0$ genügt, so liefern diese Potenzen alle Wurzeln der Gleichung $x^n - 1 = 0$.

Diese Schlüsse würden nicht gelten, wenn k einen gemeinsamen Theiler mit n hätte. Ist nämlich ν ein solcher gemeinsamer Theiler, dann würde $k \cdot \frac{n}{\nu}$ durch n theilbar, und folglich eine niedrigere Potenz als r^n, nämlich $r^{\frac{n}{\nu}}$ der Einheit gleich. In diesem Falle können die Potenzen von r höchstens $\frac{n}{\nu}$ Wurzeln der Gleichung $x^n - 1 = 0$ liefern, und zwar werden es in der That so viele Wurzeln, wenn ν der grösste gemeinsame Theiler der Zahlen k, n ist. In unserem Falle, in dem k und n als theilerfremd angenommen sind, wird man

passend von einer **primitiven** Wurzel*) der Gleichung $x^n - 1 = 0$ reden; dagegen in dem anderen Falle, in welchem k und n als (grössten) gemeinsamen Theiler ν haben, soll r eine **nichtprimitive** Wurzel jener Gleichung genannt werden; es ist klar, dass dann r eine primitive Wurzel der Gleichung $x^{\frac{n}{\nu}} - 1 = 0$ werden würde. Die einfachste nichtprimitive Wurzel ist die Einheit; im Falle n eine Primzahl ist, giebt es weiter keine nichtprimitiven Wurzeln.

§ 12. Setzen wir nun

$$W = 1 + r + r^4 + r^9 + \cdots + r^{(n-1)^2},$$

so wird offenbar $W = T + iU$, so dass T der reelle Theil von W ist und U aus dem imaginären Theile von W durch Unterdrückung des Factors i hervorgeht. Unsere gesammte Aufgabe reducirt sich daher auf die Bestimmung der Summe W. Zu diesem Zwecke kann sowohl die in § 6 betrachtete, wie die in § 9 summirte Reihe verwendet werden. Für den Fall, dass n gerade ist, wird die erste weniger geeignet sein. Trotzdem wird es, wie wir hoffen, dem Leser angenehm sein, wenn wir den Fall, in welchem n ungerade ist, nach beiden Methoden behandeln.

Wir wollen also zunächst voraussetzen, n sei eine ungerade Zahl; r bezeichne irgend eine primitive Wurzel der Gleichung $x^n - 1 = 0$. In $f(x, m)$ setzen wir $x = r$ und $m = n - 1$. Das giebt offenbar

$$\frac{1 - x^m}{1 - x} = \frac{1 - r^{-1}}{1 - r} = - r^{-1},$$

$$\frac{1 - x^{m-1}}{1 - x^2} = \frac{1 - r^{-2}}{1 - r^2} = - r^{-2},$$

$$\frac{1 - x^{m-2}}{1 - x^3} = \frac{1 - r^{-3}}{1 - r^3} = - r^{-3}, \ldots$$

bis zu

$$\frac{1 - x}{1 - x^m} = \frac{1 - r^{-m}}{1 - r^m} = - r^{-m}.$$

(Es wird nicht überflüssig sein, daran zu erinnern, dass diese Gleichungen nur so lange gelten, als r eine primitive Wurzel

*) *Gauss* gebraucht die Bezeichnung »radix propria« und »impropria«. Wir haben die jetzt allgemein üblichen Benennungen »primitiv« und »nichtprimitiv« beibehalten.

ist; wäre nämlich r eine nichtprimitive Wurzel, dann würden mehrere der Brüche unbestimmt werden, da Zähler und Nenner derselben gleichzeitig verschwinden).

Hieraus leiten wir die folgende Gleichung ab

$$f(r, n-1) = 1 + r^{-1} + r^{-3} + r^{-6} + \cdots + r^{-\frac{1}{2}(n-1)n}$$
$$= (1 - r)(1 - r^{3})(1 - r^{5}) \ldots (1 - r^{n-2}).$$

Dieselbe Gleichung wird auch dann gelten, wenn r^{λ} für r eingesetzt wird, wobei λ irgend eine ganze, zu n theilerfremde Zahl bedeutet, weil dann auch r^{λ} eine primitive Wurzel der Gleichung $x^{n} - 1 = 0$ wird. Schreiben wir also r^{n-2} oder, was das Gleiche ist, r^{-2} statt r, so wird

$$1 + r^{2} + r^{6} + r^{12} + \cdots + r^{(n-1)n}$$
$$= (1 - r^{-2})(1 - r^{-6})(1 - r^{-10}) \ldots (1 - r^{-2(n-2)}).$$

Beide Seiten dieser Gleichung multipliciren wir mit

$$r \,.\, r^{3} \,.\, r^{5} \ldots r^{n-2} = r^{\frac{1}{4}(n-1)^{2}},$$

dann entsteht, wegen

$$r^{2 + \frac{1}{4}(n-1)^{2}} = r^{\frac{1}{4}(n-3)^{2}}, \qquad r^{(n-1)n + \frac{1}{4}(n-1)^{2}} = r^{\frac{1}{4}(n+1)^{2}},$$
$$r^{6 + \frac{1}{4}(n-1)^{2}} = r^{\frac{1}{4}(n-5)^{2}}, \qquad r^{(n-2)(n-1) + \frac{1}{4}(n-1)^{2}} = r^{\frac{1}{4}(n+3)^{2}},$$
$$r^{12 + \frac{1}{4}(n-1)^{2}} = r^{\frac{1}{4}(n-7)^{2}}, \qquad r^{(n-3)(n-2) + \frac{1}{4}(n-1)^{2}} = r^{\frac{1}{4}(n+5)^{2}}, \ldots$$

die folgende Gleichung

$$r^{\frac{1}{4}(n-1)^{2}} + r^{\frac{1}{4}(n-3)^{2}} + r^{\frac{1}{4}(n-5)^{2}} + \cdots + r + 1$$
$$+ r^{\frac{1}{4}(n+1)^{2}} + r^{\frac{1}{4}(n+3)^{2}} + r^{\frac{1}{4}(n+5)^{2}} + \cdots + r^{\frac{1}{4}(2n-2)^{2}}$$
$$= (r - r^{-1})(r^{3} - r^{-3})(r^{5} - r^{-5}) \ldots (r^{n-2} - r^{-n+2})$$

oder bei anderer Anordnung der Glieder auf der linken Seite

$$(5) \quad 1 + r + r^{4} + \cdots + r^{(n-1)^{2}}$$
$$= (r - r^{-1})(r^{3} - r^{-3})(r^{5} - r^{-5}) \ldots (r^{n-2} - r^{-n+2})$$

§ 13. Die Factoren der rechten Seite in (5) lassen sich auch folgendermaassen darstellen

$$r - r^{-1} = -(r^{n-1} - r^{-n+1}),$$
$$r^{3} - r^{-3} = -(r^{n-3} - r^{-n+3}),$$
$$r^{5} - r^{-5} = -(r^{n-5} - r^{-n+5}), \ldots$$

bis zu

$$r^{n-2} - r^{-n+2} = -(r^{2} - r^{-2});$$

dadurch nimmt jene Gleichung die Form an

$$W = (-1)^{\frac{1}{2}(n-1)} (r^2 - r^{-2}) (r^4 - r^{-4}) (r^6 - r^{-6}) \ldots (r^{n-1} - r^{-n+1}).$$

Multiplicirt man diese Gleichung mit der ursprünglichen Form von (5), so ergiebt sich

$$W^2 = (-1)^{\frac{1}{2}(n-1)} (r - r^{-1}) (r^2 - r^{-2}) (r^3 - r^{-3}) \ldots (r^{n-1} - r^{-n+1}),$$

wobei $(-1)^{\frac{1}{2}(n-1)}$ gleich $+1$ oder gleich -1 ist, je nachdem n die Form $4\mu + 1$ oder $4\mu + 3$ besitzt. Folglich ist

$$W^2 = \pm r^{\frac{1}{2}n(n-1)} (1 - r^{-2}) (1 - r^{-4}) (1 - r^{-6}) \ldots (1 - r^{-2(n-1)}).$$

Man erkennt ohne Mühe, dass r^{-2}, r^{-4}, r^{-6}, $\ldots$ r^{-2n+2} alle Wurzeln der Gleichung $x^n - 1 = 0$ liefern, ausgenommen die Wurzel $x = 1$; folglich muss die Gleichung stattfinden

$$(x - r^{-2}) (x - r^{-4}) (x - r^{-6}) \cdots (x - r^{-2n+2}) \\ = x^{n-1} + x^{n-2} + x^{n-3} + \cdots + x + 1,$$

und hieraus wird für $x = 1$

$$(1 - r^{-2}) (1 - r^{-4}) (1 - r^{-6}) \cdots (1 - r^{-2n+2}) = n.$$

Da ferner offenbar $r^{\frac{1}{2}n(n-1)} = 1$ wird, so geht unsere Gleichung über in

$$(6) \qquad W^2 = \pm n.$$

Im Falle, dass n die Form $4\mu + 1$ hat, wird

$$W = \pm \sqrt{n} \quad \text{und daher} \quad T = \pm \sqrt{n}, \quad U = 0;$$

dagegen in dem anderen Falle, in welchem n die Form $4\mu + 3$ hat,

$$W = \pm i \sqrt{n} \quad \text{und daher} \quad T = 0, \quad U = \pm \sqrt{n}.$$

§ 14. Die Methode des vorhergehenden Artikels giebt nur den absoluten Werth der Aggregate T und U, und lässt es zweifelhaft, ob man T im ersten und U im zweiten Falle $= +\sqrt{n}$ oder $= -\sqrt{n}$ setzen muss. Dies lässt sich nun, wenigstens für den Fall $k = 1$ aus der Gleichung (5) auf folgende Art bestimmen. Da man für $k = 1$ hat

$$r - r^{-1} = 2i \sin \omega,$$
$$r^3 - r^{-3} = 2i \sin 3\omega,$$
$$r^5 - r^{-5} = 2i \sin 5\omega, \ldots$$

so wandelt sich jene Gleichung um in

$$W = (2i)^{\frac{1}{2}(n-1)} \sin \omega \sin 3\omega \sin 5\omega \ldots \sin (n-2)\omega.$$

Nun giebt es in dem Falle, dass n die Form $4\mu + 1$ hat, in der Reihe der ungeraden Zahlen

$$1, 3, 5, 7, \ldots \tfrac{1}{2}(n-3), \tfrac{1}{2}(n+1), \ldots (n-2)$$

$\frac{1}{4}(n-1)$, welche kleiner als $\frac{1}{2}n$ sind, und diesen entsprechen offenbar positive Sinus; die übrigen $\frac{1}{4}(n-1)$ dagegen sind grösser als $\frac{1}{2}n$, und diesen entsprechen negative Sinus. Deswegen ist das Product aller Sinus gleich dem Producte aus einer positiven Grösse in den Multiplicator $(-1)^{\frac{1}{4}(n-1)}$, und also wird W gleich dem Producte aus einer reellen positiven Grösse in i^{n-1}, d. h. in 1, weil ja $i^4 = 1$ und $n-1$ durch 4 theilbar ist. Demnach ist W eine reelle, positive Grösse, so dass nothwendig sein muss

$$W = +\sqrt{n}, \quad T = +\sqrt{n}.$$

Im anderen Falle, in dem n die Form $4\mu + 3$ hat, werden in der Reihe der ungeraden Zahlen

$$1, 3, 5, 7, \ldots \tfrac{1}{2}(n-1), \tfrac{1}{2}(n+3), \ldots (n-2)$$

die ersten $\frac{1}{4}(n+1)$ kleiner als $\frac{1}{2}n$ und die übrigen $\frac{1}{4}(n-3)$ grösser als $\frac{1}{2}n$. Folglich werden unter den Sinus der Bogen $\omega, 3\omega, 5\omega, \ldots (n-2)\omega$ genau $\frac{1}{4}(n-3)$ negativ werden, und also wird W das Product aus $i^{\frac{1}{2}(n-1)}$ in eine reelle positive Grösse und in $(-1)^{\frac{1}{4}(n-3)}$. Der dritte Factor ist $i^{\frac{1}{2}(n-3)}$; er liefert mit dem ersten verbunden $i^{n-2} = i$, da ja $i^{n-3} = 1$ ist. Folglich wird nothwendigerweise

$$W = +i\sqrt{n} \quad \text{und} \quad T = +\sqrt{n}.$$

§ 15. Wir zeigen nun, auf welche Weise dieselben Schlüsse aus der in § 9 betrachteten Reihe hergeleitet werden können. Schreiben wir $-y^{-1}$ statt $x^{\frac{1}{2}}$ in der Gleichung (4), dann wird

$$1 - y^{-1}\frac{1-y^{-2m}}{1-y^{-2}} + y^{-2}\frac{(1-y^{-2m})(1-y^{-2m+2})}{(1-y^{-2})(1-y^{-4})}$$

$$- y^{-3}\frac{(1-y^{-2m})(1-y^{-2m+2})(1-y^{-2m+4})}{(1-y^{-2})(1-y^{-4})(1-y^{-6})} + \ldots$$

(7) u. s. w. bis zum $(m+1)^{\text{ten}}$ Gliede

$$= (1-y^{-1})(1+y^{-2})(1-y^{-3})(1+y^{-4}) \ldots (1 \pm y^{-m}).$$

Nimmt man nun für y eine primitive Wurzel der Gleichung $y^n - 1 = 0$ an, die wir gleich r setzen, und nimmt man gleichzeitig $m = n - 1$, so wird

$$\frac{1 - y^{-2m}}{1 - y^{-2}} = \frac{1 - r^2}{1 - r^{-2}} = - r^2,$$
$$\frac{1 - y^{-2m+2}}{1 - y^{-4}} = \frac{1 - r^4}{1 - r^{-4}} = - r^4,$$
$$\frac{1 - y^{-2m+4}}{1 - y^{-6}} = \frac{1 - r^6}{1 - r^{-6}} = - r^6, \ldots$$

bis zu

$$\frac{1 - y^{-2}}{1 - y^{-2m}} = \frac{1 - r^{2n-2}}{1 - r^{-2n+2}} = - r^{2n-2},$$

wobei zu bemerken ist, dass keiner der Nenner $1 - r^{-2}$, $1 - r^{-4}, \ldots$ gleich 0 wird. Demnach nimmt die Gleichung (7) die Form an

$$1 + r + r^4 + r^9 + \cdots + r^{(n-1)^2}$$
$$= (1 - r^{-1})(1 + r^{-2})(1 - r^{-3}) \ldots (1 + r^{-n+1}).$$

Multipliciren wir auf der linken Seite dieser Gleichung das erste mit dem letzten Gliede, das zweite mit dem vorletzten u. s. w., dann kommen wir auf

$$(1 - r^{-1})(1 + r^{-n+1}) = r - r^{-1},$$
$$(1 + r^{-2})(1 - r^{-n+2}) = r^{n-2} - r^{-n+2},$$
$$(1 - r^{-3})(1 + r^{-n+3}) = r^3 - r^{-3},$$
$$(1 + r^{-4})(1 - r^{-n+4}) = r^{n-4} - r^{-n+4}, \ldots$$

Aus diesen Partialproducten setzt sich dann das Gesammtproduct

$$(r - r^{-1})(r^3 - r^{-3})(r^5 - r^{-5}) \ldots (r^{n-4} - r^{-n+4})(r^{n-2} - r^{-n+2})$$

zusammen, und dies wird also

$$= 1 + r + r^4 + r^9 + \cdots + r^{(n-1)^2} = W.$$

Diese Gleichung ist mit der § 12, (5) aus der ersten Reihe abgeleiteten identisch; es können an sie die übrigen Schlüsse wie in den § 13 und § 14 geknüpft werden.

§ 16. Wir gehen nun zu dem anderen Falle über, in welchem n eine gerade Zahl ist. Sie sei zunächst von der Form $4\mu + 2$ oder ungerade mal gerade, dann ist es offenbar, dass die Zahlen $\frac{1}{4} n^2$, $(\frac{1}{2} n + 1)^2 - 1$, $(\frac{1}{2} n + 2)^2 - 4, \ldots$

und allgemein $(\frac{1}{2}n + \lambda)^2 - \lambda^2$ durch $\frac{1}{2}n$ dividirt ungerade Quotienten geben und deshalb sämmtlich modulo n congruent zu $\frac{1}{2}n$ sein werden. Demnach wird, wenn r eine primitive Wurzel der Gleichung $x^n - 1 = 0$ und also $r^{\frac{1}{2}n} = -1$ ist,

$$r^{(\frac{1}{2}n)^2} = -1, \quad r^{(\frac{1}{2}n+1)^2} = -r, \quad r^{(\frac{1}{2}n+2)^2} = -r^4,$$
$$r^{(\frac{1}{2}n+3)^2} = -r^9, \ldots$$

Daraus folgt, dass in der Reihe

$$1 + r + r^4 + r^9 + \cdots + r^{(n-1)^2}$$

das Glied $r^{(\frac{1}{2}n)^2}$ durch das erste Glied zerstört wird, das folgende Glied durch das zweite; u. s. f.; und so wird

$$W = 0, \quad T = 0, \quad V = 0.$$

§ 17. Es bleibt nur der Fall noch übrig, dass n von der Form 4μ, d. h. gerade mal gerade wird. Hierfür wird allgemein $(\frac{1}{2}n + \lambda)^2 - \lambda^2$ durch n theilbar werden, und sonach gilt

$$r^{(\frac{1}{2}n+\lambda)^2} = r^{\lambda^2}.$$

Daraus folgt, dass in der Reihe

$$1 + r + r^4 + r^9 + \cdots + r^{(n-1)^2}$$

das Glied $r^{(\frac{1}{2}n)^2}$ dem ersten gleich wird, das folgende Glied dem zweiten u. s. f., so dass man erhält

$$W = 2\,(1 + r + r^4 + r^9 + \cdots + r^{(\frac{1}{2}n-1)^2}).$$

Jetzt nehmen wir in § 15, (7) $m = \frac{1}{2}n - 1$ an und setzen für y eine primitive Wurzel der Gleichung $y^n - 1 = 0$, die r heissen möge. Dann erhält man genau wie in § 15 eine Gleichung von folgender Form

$$1 + r + r^4 + r^9 + \cdots + r^{(\frac{1}{2}n-1)^2}$$
$$= (1 - r^{-1})(1 + r^{-2})(1 - r^{-3}) \ldots (1 - r^{-\frac{1}{2}n+1})$$

d. h.

$$(8)\quad W = 2(1 - r^{-1})(1 + r^{-2})(1 - r^{-3})(1 + r^{-4}) \ldots (1 - r^{-\frac{1}{2}n+1}).$$

Da ferner $r^{\frac{1}{2}n} = -1$ ist, so wird

$$1 + r^{-2} = -r^{\frac{1}{2}n-2}(1 - r^{-\frac{1}{2}n+2}),$$
$$1 + r^{-4} = -r^{\frac{1}{2}n-4}(1 - r^{-\frac{1}{2}n+4}),$$
$$1 + r^{-6} = -r^{\frac{1}{2}n-6}(1 - r^{-\frac{1}{2}n+6}), \ldots;$$

weiter wird das Product aus den Factoren $-r^{\frac{1}{2}n-2}$, $-r^{\frac{1}{2}n-4}$, $-r^{\frac{1}{2}n-6}$, ... $-r^2$ gleich $(-1)^{\frac{1}{4}n-1} r^{\frac{1}{16}n^2 - \frac{1}{4}n}$, so dass die

vorhergehende Gleichung auch folgendermaassen geschrieben werden kann:

$$W = 2(-1)^{\frac{1}{4}n-1}\, r^{\frac{1}{16}n^2 - \frac{1}{4}n}(1 - r^{-1})(1 - r^{-2})(1 - r^{-3}) \dots$$
$$\dots (1 - r^{-\frac{1}{2}n+1}).$$

Da nun

$$1 - r^{-1} = -r^{-1}(1 - r^{-n+1}),$$
$$1 - r^{-2} = -r^{-2}(1 - r^{-n+2}),$$
$$1 - r^{-3} = -r^{-3}(1 - r^{-n+3}), \dots$$

ist, so wird

$$(1 - r^{-1})(1 - r^{-2})(1 - r^{-3}) \dots (1 - r^{-\frac{1}{2}n+1}) \dots$$
$$= (-1)^{\frac{1}{2}n-1}\, r^{-\frac{1}{8}n^2 + \frac{1}{4}n}(1 - r^{-\frac{1}{2}n-1})(1 - r^{-\frac{1}{2}n-2})$$
$$(1 - r^{-\frac{1}{2}n-3}) \dots (1 - r^{-n+1}),$$

und folglich

$$W = 2(-1)^{\frac{3}{4}n-2}\, r^{\frac{1}{16}n^2}(1 - r^{-\frac{1}{2}n-1})(1 - r^{-\frac{1}{2}n-2})$$
$$(1 - r^{-\frac{1}{2}n-3}) \dots (1 - r^{-n+1}).$$

Multipliciren wir nun diesen Werth von W mit dem früher gefundenen und fügen auf beiden Seiten den Factor $1 - r^{-\frac{1}{2}n}$ hinzu, dann entsteht

$$(1 - r^{-\frac{1}{2}n})W^2 = 4(-1)^{n-3}\, r^{-\frac{1}{4}n}(1 - r^{-1})(1 - r^{-2})$$
$$(1 - r^{-3}) \dots (1 - r^{-n+1}).$$

Nun ist aber

$$1 - r^{-\frac{1}{2}n} = 2, \quad (-1)^{n-3} = -1, \quad r^{-\frac{1}{4}n} = -r^{+\frac{1}{4}n},$$
$$(1 - r^{-1})(1 - r^{-2})(1 - r^{-3}) \dots (1 - r^{-n+1}) = n.$$

und daher schliesslich

$$W^2 = 2r^{\frac{1}{4}n}n. \tag{9}$$

Man erkennt leicht, dass $r^{\frac{1}{4}n}$ entweder $= +i$ oder $= -i$ ist, je nachdem k von der Form $4\mu + 1$ oder von der Form $4\mu + 3$ wird. Da weiter

$$2i = (1 + i)^2, \quad -2i = (1 - i)^2$$

ist, so hat man in dem Falle, dass k von der Form $4\mu + 1$ wird,

$$W = \pm(1 + i)\sqrt{n} \text{ und also } T = U = \pm\sqrt{n};$$

im anderen Falle aber, dass k von der Form $4\mu + 3$ wird,

$$W = \pm(1 - i)\sqrt{n} \text{ und also } T = -U = \pm\sqrt{n}.$$

§ 18. Die Methode des vorigen Paragraphen hat uns die absoluten Werthe der Functionen T und U geliefert und die Bedingungen aufgezeigt, unter denen ihnen gleiche oder verschiedene Vorzeichen gegeben werden müssen; aber die Zeichen selbst werden auf diesem Wege noch nicht bestimmt. Wir können dies für den Fall $k = 1$ auf folgende Art ergänzen.

Setzen wir $\varrho = \cos \frac{1}{2}\omega + i \sin \frac{1}{2}\omega$, so dass $r = \varrho^2$ wird, dann folgt, dass man wegen $\varrho^n = -1$ die Gleichung (8) so schreiben kann

$$W = 2(1 + \varrho^{n-2})(1 + \varrho^{-4})(1 + \varrho^{n-6})(1 + \varrho^{-8}) \dots$$
$$\dots (1 + \varrho^{-n+4})(1 + \varrho^2)$$

Nun wird

$$\begin{aligned} 1 + \varrho^2 &= 2\varrho \cos \tfrac{1}{2}\omega, \\ 1 + \varrho^{-4} &= 2\varrho^{-2} \cos \omega, \\ 1 + \varrho^{+6} &= 2\varrho^3 \cos \tfrac{3}{2}\omega, \\ 1 + \varrho^{-8} &= 2\varrho^{-4} \cos 2\omega, \dots \end{aligned}$$

bis zu

$$\begin{aligned} 1 + \varrho^{-n+4} &= 2\varrho^{-\frac{1}{2}n+2} \cos (\tfrac{1}{4}n - 1)\omega, \\ 1 + \varrho^{n-2} &= 2\varrho^{\frac{1}{2}n-1} \cos (\tfrac{1}{4}n - \tfrac{1}{2})\omega; \end{aligned}$$

und daher hat man

$$W = 2^{\frac{1}{2}n} \varrho^{\frac{1}{4}n} \cos \tfrac{1}{2}\omega \cos \omega \cos \tfrac{3}{2}\omega \dots \cos (\tfrac{1}{4}n - \tfrac{1}{2})\omega.$$

Alle Cosinus, welche in dieses Product eingehen, sind offenbar positiv, und der Factor $\varrho^{\frac{1}{4}n}$ wird $= \cos 45^0 + i \sin 45^0 = (1 + i)\sqrt{\frac{1}{2}}$. Daraus schliessen wir, dass W das Product aus $1 + i$ in eine reelle positive Grösse ist; daher muss nothwendigerweise werden

$$W = (1 + i)\sqrt{n}, \quad T = +\sqrt{n}, \quad U = +\sqrt{n}.$$

§ 19. Es ist der Mühe werth, alle bisher entwickelten Summen in einer Tafel zusammenzustellen. Es ist also ganz allgemein

$T =$	$U =$	falls n von der Form ist
$\pm\sqrt{n}$	$\pm\sqrt{n}$	4μ,
$\pm\sqrt{n}$	0	$4\mu + 1$,
0	0	$4\mu + 2$,
0	$\pm\sqrt{n}$	$4\mu + 3$,

und in dem Falle, in welchem $k = 1$ genommen wird, muss der Wurzelgrösse das positive Vorzeichen zuertheilt werden.

Es ist somit das, was für Primzahlwerthe von n im § 3 durch Induction erlangt worden ist, in aller Strenge bewiesen worden, und es bleibt nur übrig zu zeigen, wie in allen Fällen für beliebige Werthe von k die Zeichen bestimmt werden. Bevor wir an diese ganz allgemeine Aufgabe herantreten, müssen wir zunächst die Fälle, in denen n eine Primzahl oder eine Primzahlpotenz ist, näher betrachten.

§ 20. Zunächst sei n eine ungerade Primzahl: aus dem in § 10 Dargelegten erhellt, dass $W = 1 + 2\Sigma r^a = 1 + 2\Sigma R^{ak}$ ist, wenn $R = \cos\omega + i\sin\omega$, und a, wie dort, unbestimmt alle quadratischen Reste von n bedeutet, die zwischen 1 und $n - 1$ liegen. Bezeichnen wir ferner durch b unbestimmt alle quadratischen Nichtreste von n zwischen denselben Grenzen, so erkennt man ohne Mühe, dass alle Zahlen ak modulo n entweder allen a oder allen b (abgesehen von der Zuordnung) congruent sein werden, je nachdem k ein Rest oder ein Nichtrest ist. Demnach wird im ersten Falle

$$W = 1 + 2\Sigma R^a = 1 + R + R^4 + R^9 + \cdots + R^{(n-1)^2}$$

und somit $W = +\sqrt{n}$, wenn n von der Form $4\mu + 1$, dagegen $W = +i\sqrt{n}$, wenn n von der Form $4\mu + 3$ ist.

Im anderen Falle dagegen wird, wenn k Nichtrest von n ist,

$$W = 1 + 2\Sigma R^b.$$

Da nun offenbar alle Zahlen a, b den Gesammtcomplex der Zahlen 1, 2, 3, ... ausmachen, und da also

$$\Sigma R^a + \Sigma R^b = R + R^2 + R^3 + \cdots + R^{n-1} = -1$$

ist, so wird

$$W = -1 - 2\Sigma R^a = -(1 + R + R^4 + R^9 + \cdots + R^{(n-1)^2})$$

und somit $W = -\sqrt{n}$, wenn n von der Form $4\mu + 1$, und $W = -i\sqrt{n}$, wenn n von der Form $4\mu + 3$ ist.

Unsere Resultate sind:

erstens, wenn n die Form $4\mu + 1$ hat, und k quadratischer Rest von n ist,

$$T = +\sqrt{n}, \quad U = 0;$$

zweitens, wenn n die Form $4\mu + 1$ hat, und k Nichtrest von n ist,

$$T = -\sqrt{n}, \quad U = 0;$$

drittens, wenn n die Form $4\mu + 3$ hat, und k Rest von n ist,

$$T = 0, \quad U = +\sqrt{n};$$

viertens, wenn n die Form $4\mu + 3$ hat, und k Nichtrest von n ist,

$$T = 0, \quad U = -\sqrt{n}.$$

§ 21. Es sei ferner n das Quadrat oder eine höhere Potenz der ungeraden Primzahl p; wir setzen $n = p^{2\varkappa}q$, so dass q entweder $= 1$ oder $= p$ ist. Hier ist vor Allem zu beachten, dass, wenn λ irgend welche, durch $p^\varkappa$ nicht theilbare Zahl ist, dann

$$r^{\lambda^2} + r^{(\lambda + p^\varkappa q)^2} + r^{(\lambda + 2p^\varkappa q)^2} + r^{(\lambda + 3p^\varkappa q)^2} + \cdots + r^{(\lambda + n - p^\varkappa q)^2}$$
$$= r^{\lambda^2}\left\{1 + r^{2\lambda p^\varkappa q} + r^{4\lambda p^\varkappa q} + r^{6\lambda p^\varkappa q} + \cdots + r^{2\lambda(n - p^\varkappa q)}\right\}$$
$$= \frac{r^{\lambda^2}\left(1 - r^{2\lambda n}\right)}{1 - r^{2\lambda p^\varkappa q}} = 0$$

wird. Hieraus erkennt man leicht, dass man

$$W = 1 + r^{p^{2\varkappa}} + r^{4p^{2\varkappa}} + r^{9p^{2\varkappa}} + \cdots + r^{(n - p^\varkappa)^2}$$

hat. Es können nämlich die übrigen Glieder der Reihe

$$1 + r + r^4 + r^9 + \cdots + r^{(n-1)^2}$$

in $(p^\varkappa - 1)q$ partielle Reihen vertheilt werden, welche je $p^\varkappa$ Glieder enthalten und gemäss der eben behandelten Transformation verschwindende Summen haben.

Hieraus folgt in dem Falle, dass $q = 1$ d. h. dass n eine Primzahlpotenz mit geraden Exponenten ist,

$$W = p^\varkappa = +\sqrt{n} \quad \text{und also} \quad T = +\sqrt{n}, \quad U = 0.$$

Dagegen setzen wir in dem Falle, dass $q = p$, d. h. wenn n eine Primzahlpotenz mit ungeraden Exponenten ist, $r^{p^{2\varkappa}} = \varrho$; dann wird ϱ eine primitive Wurzel der Gleichung $x^p - 1 = 0$ und zwar $\varrho = \cos\frac{k}{p}\,360^\circ + i\sin\frac{k}{p}\,360^\circ$; folglich ist

$$W = 1 + \varrho + \varrho^4 + \varrho^9 + \cdots + \varrho^{(p^{\varkappa+1} - 1)^2}$$
$$= p^\varkappa\left(1 + \varrho + \varrho^4 + \cdots + \varrho^{(p-1)^2}\right).$$

Nun wird die Summe der Reihe $1 + \varrho + \varrho^4 + \varrho^9 + \cdots + \varrho^{(p-1)^2}$ durch den vorhergehenden Paragraphen bestimmt. Daraus fliesst sofort

$$W = \pm\sqrt{n} = V, \text{ wenn } p \text{ die Form } 4\mu + 1 \text{ hat.}$$
$$W = \pm i\sqrt{n} = iV, \text{ wenn } p \text{ die Form } 4\mu + 3 \text{ hat;}$$

dabei gilt das positive oder das negative Vorzeichen, je nachdem k Rest oder Nichtrest von p ist.

§ 22. Leicht ergiebt sich auch aus dem in § 20 und 21 Dargelegten folgender Satz, der uns unten von wesentlichem Nutzen sein wird. Wir setzen

$$W' = 1 + r^h + r^{4h} + r^{9h} + \cdots + r^{h(n-1)^2},$$

wobei h irgend eine ganze, durch p nicht theilbare Zahl bedeutet; dann wird in dem Falle, in welchem $n = p$ oder eine ungerade Potenz von p ist,

$$W' = W, \text{ wenn } h \text{ quadratischer Rest von } p \text{ ist.}$$
$$W' = -W, \text{ wenn } h \text{ quadratischer Nichtrest von } p \text{ ist.}$$

Denn offenbar entsteht W' aus W, wenn kh für k eingesetzt wird. Im ersten Falle sind hinsichtlich des Charakters als Reste oder Nichtreste von p die Zahlen k und kh einander gleichartig, im zweiten aber ungleichartig.

In dem Falle jedoch, in welchem n eine gerade Potenz von p ist, wird offenbar $W' = +\sqrt{n}$, und also stets $W' = W$.

§ 23. In den §§ 20, 21, 22 haben wir ungerade Primzahlen und deren Potenzen betrachtet; es bleibt noch der Fall übrig, dass n eine Potenz von 2 ist.

Für $n = 2$ ist offenbar $W = 1 + r = 0$.

Für $n = 4$ ergiebt sich $W = 1 + r + r^4 + r^9 = 2 + 2r$, und folglich $W = 2 + 2i$, falls k die Form $4\mu + 1$ hat, und $W = 2 - 2i$, falls k die Form $4\mu + 3$ hat.

Für $n = 8$ haben wir $W = 1 + r + r^4 + r^9 + r^{16} + r^{25} + r^{36} + r^{49} = 2 + 4r + 2r^4 = 4r$. Folglich wird

$$W = (1 + i)\sqrt{8}; \text{ falls } k \text{ die Form } 8\mu + 1 \text{ hat.}$$
$$W = (-1 + i)\sqrt{8}; \text{ falls } k \text{ die Form } 8\mu + 3 \text{ hat.}$$
$$W = (-1 - i)\sqrt{8}; \text{ falls } k \text{ die Form } 8\mu + 5 \text{ hat.}$$
$$W = (1 - i)\sqrt{8}; \text{ falls } k \text{ die Form } 8\mu + 7 \text{ hat.}$$

Ist n eine höhere Potenz von 2, so setzen wir $n = 2^{2\varkappa} q$, so dass q entweder $= 1$ oder $= 2$, und $\varkappa > 1$ wird. Hier ist vor Allem zu beachten, dass, wenn λ irgend eine ganze durch $2^{\varkappa - 1}$ nicht theilbare ganze Zahl ist, dann

$$r^{\lambda^2} + r^{(\lambda + 2^{\chi} q)^2} + r^{(\lambda + 2 \cdot 2^{\chi} q)^2} + r^{(\lambda + 3 \cdot 2^{\chi} q)^2} + \cdots + r^{(\lambda + n - 2^{\chi} q)^2}$$
$$= r^{\lambda^2} \{ 1 + r^{2^{\chi+1} \lambda q} + r^{2 \cdot 2^{\chi+1} \lambda q} + r^{3 \cdot 2^{\chi+1} \lambda q} + \cdots + r^{(2n - 2^{\chi+1} q) \lambda} \}$$
$$= \frac{r^{\lambda^2} (1 - r^{2 \lambda n})}{1 - r^{2^{\chi+1} \lambda q}} = 0$$

wird. Hieraus erkennt man ohne Schwierigkeit, dass man hat

$$W = 1 + r^{2^{2\chi-2}} + r^{4 \cdot 2^{2\chi-2}} + r^{9 \cdot 2^{2\chi-2}} + \cdots + r^{(n - 2^{\chi-1})^2}.$$

Setzen wir $r^{2^{2\chi-2}} = \varrho$, dann wird ϱ eine Wurzel der Gleichung $x^{4q} - 1 = 0$, und zwar

$$\varrho = \cos \frac{k}{4q} 360^0 + i \sin \frac{k}{4q} 360^0.$$

Hieraus folgt

$$W = 1 + \varrho + \varrho^4 + \varrho^9 + \cdots + \varrho^{(2^{\chi+1} q - 1)^2}$$
$$= 2^{\chi-1} (1 + \varrho + \varrho^4 + \varrho^9 + \cdots + \varrho^{(4q-1)^2}).$$

Nun wird die Summe der Reihe $1 + \varrho + \varrho^4 + \varrho^9 + \ldots + \varrho^{(4q-1)^2}$ durch die Resultate für $n = 4$ und $n = 8$ bestimmt. Daraus schliessen wir bei $q = 1$, d. h. wenn n eine Potenz von 4 ist,

$W = (1 + i) 2^{\chi} = (1 + i) \sqrt{n}$, wenn k die Form $4\mu + 1$ hat,
$W = (1 - i) 2^{\chi} = (1 - i) \sqrt{n}$, wenn k die Form $4\mu + 3$ hat;

dies sind ganz genau die Formeln, welche für $n = 4$ gelten.

In dem Falle jedoch, dass $q = 2$, d. h. dass n eine Potenz von 2 mit einem ungeraden Exponenten > 3 ist, erhält man

$W = \quad (1 + i) 2^{\chi} \sqrt{2} = \quad (1 + i) \sqrt{n}$, wenn k von der Form $8n + 1$ ist,
$W = (-1 + i) 2^{\chi} \sqrt{2} = (-1 + i) \sqrt{n}$, wenn k von der Form $8n + 3$ ist,
$W = (-1 - i) 2^{\chi} \sqrt{2} = (-1 - i) \sqrt{n}$, wenn k von der Form $8n + 5$ ist,
$W = \quad (1 - i) 2^{\chi} \sqrt{2} = \quad (1 - i) \sqrt{n}$, wenn k von der Form $8n + 7$ ist;

Dies stimmt völlig mit dem für $n = 8$ Abgeleiteten überein.

§ 24. Hier wird es gleichfalls der Mühe werth sein, das Verhältniss der Reihen-Summe

$$W' = 1 + r^h + r^{4h} + r^{9h} + \cdots + r^{h(n-1)^2}$$

zu W zu bestimmen, wobei h irgend eine ungerade ganze Zahl bedeutet. Da W' aus W hervorgeht, wenn man k in kh verwandelt, so wird W' genau so von der Form der Zahl kh abhängen, wie W von der Form der Zahl k. Setzen wir $W' : W = l$, so ist klar:

I. in dem Falle $n = 4$ oder wenn n eine höhere gerade Potenz von 2 ist, wird

$l = 1$, wenn h die Form $4\mu + 1$,
$l = -i$, wenn h die Form $4\mu + 3$, und k die Form $4\mu + 1$,
$l = +i$, wenn h die Form $4\mu + 3$, und k dieselbe Form hat;

II. in dem Falle $n = 8$ oder wenn n eine höhere ungerade Potenz von 2 ist, wird

$l = 1$, wenn h die Form $8\mu + 1$,
$l = -1$, wenn h die Form $8\mu + 5$,
$l = +i$, wenn entweder h die Form $8\mu + 3$, und k die Form $4\mu + 1$, oder h die Form $8\mu + 7$, und k die Form $4\mu + 3$,
$l = -i$, wenn entweder h die Form $8\mu + 3$, und k die Form $4\mu + 3$, oder h die Form $8\mu + 7$, und k die Form $4\mu + 1$ hat.

Hierdurch ist die vollständige Bestimmung der Summe W für alle Fälle, in denen n eine Primzahl oder eine Primzahlpotenz ist, geleistet; es bleiben also nur noch die Fälle zu erledigen, in denen n aus mehreren Primzahlen zusammengesetzt ist. Hierfür bahnt uns der folgende Satz den Weg.

§ 25. Lehrsatz. Es sei n das Product aus zwei ganzen zu einander theilerfremden Zahlen a und b, und es werde gesetzt

$$P = 1 + r^{a^2} + r^{4a^2} + r^{9a^2} + \cdots + r^{(b-1)^2 a^2},$$
$$Q = 1 + r^{b^2} + r^{4b^2} + r^{9b^2} + \cdots + r^{(a-1)^2 b^2},$$

dann wird $W = PQ$.

Beweis. α möge unbestimmt die Zahlen $0, 1, 2, 3, \ldots a-1$, und β unbestimmt die Zahlen $0, 1, 2, 3, \ldots b-1$, endlich ν unbestimmt die Zahlen $0, 1, 2, 3, \ldots n-1$ bedeuten, dann ist offenbar

$$P = \Sigma r^{a^2 \beta^2}, \quad Q = \Sigma r^{b^2 \alpha^2}, \quad W = \Sigma r^{\nu^2}.$$

Folglich wird $PQ = \Sigma r^{a^2\beta^2 + b^2\alpha^2}$, indem man für α und β alle möglichen auf jede Weise mit einander combinirten Werthe

einsetzt. Ferner wird wegen $2ab\alpha\beta = 2n\alpha\beta$ das Product $PQ = \Sigma r^{(a\beta+b\alpha)^2}$. Nun erkennt man ohne Mühe, dass die einzelnen Werthe von $a\beta + b\alpha$ unter sich verschieden und je einem Werthe von ν gleich sind. Folglich wird

$$PQ = \Sigma r^{\nu^2} = W.$$

Wir wollen übrigens anmerken, dass r^{a^2} eine primitive Wurzel von $x^b - 1 = 0$, und r^{b^2} eine primitive Wurzel von $x^a - 1 = 0$ ist.

§ 26. Ist ferner n das Product aus drei zu einander theilerfremden Zahlen a, b, c, und setzt man $bc = b_1$, so werden auch a und b_1 theilerfremd sein; folglich wird W das Product aus den Factoren

$$1 + r^{a^2} + r^{4a^2} + r^{9a^2} + \cdots + r^{(b_1-1)^2a^2},$$
$$1 + r^{b_1^2} + r^{4b_1^2} + r^{9b_1^2} + \cdots + r^{(a-1)b_1^2}.$$

Da aber r^{a^2} eine primitive Wurzel der Gleichung $x^{bc} - 1 = 0$ ist, so wird jener erste Factor selbst das Product aus

$$1 + \varrho^{b^2} + \varrho^{4b^2} + \varrho^{9b^2} + \cdots + \varrho^{(c-1)^2b^2},$$
$$1 + \varrho^{c^2} + \varrho^{4c^2} + \varrho^{9c^2} + \cdots + \varrho^{(b-1)^2c^2},$$

wenn man $r^{a^2} = \varrho$ setzt. Daraus ergiebt sich, dass W das Product der drei Factoren ist

$$1 + r^{b^2c^2} + r^{4b^2c^2} + r^{9b^2c^2} + \cdots + r^{(a-1)^2b^2c^2},$$
$$1 + r^{a^2c^2} + r^{4a^2c^2} + r^{9a^2c^2} + \cdots + r^{(b-1)^2a^2c^2},$$
$$1 + r^{a^2b^2} + r^{4a^2b^2} + r^{9a^2b^2} + \cdots + r^{(c-1)^2a^2b^2},$$

wobei $r^{b^2c^2}$, $r^{a^2c^2}$, $r^{a^2b^2}$ bezw. primitive Wurzeln der Gleichungen $x^a - 1 = 0$, $x^b - 1 = 0$, $x^c - 1 = 0$ werden.

§ 27. Hieraus schliesst man leicht allgemein, dass, wenn n das Product beliebig vieler, zu einander theilerfremder Zahlen $a, b, c, \ldots$ ist, dann W das Product aus ebenso vielen Factoren

$$1 + r^{\frac{nn}{aa}} + r^{4\frac{nn}{aa}} + r^{9\frac{nn}{aa}} + \cdots + r^{(a-1)^2\frac{nn}{aa}},$$
$$1 + r^{\frac{nn}{bb}} + r^{4\frac{nn}{bb}} + r^{9\frac{nn}{bb}} + \cdots + r^{(b-1)^2\frac{nn}{bb}},$$
$$1 + r^{\frac{nn}{cc}} + r^{4\frac{nn}{cc}} + r^{9\frac{nn}{cc}} + \cdots + r^{(c-1)^2\frac{nn}{cc}}, \ldots$$

wird, wobei $r^{\frac{nn}{aa}}$, $r^{\frac{nn}{bb}}$, $r^{\frac{nn}{cc}}, \ldots$ primitive Wurzeln der Gleichungen $x^a - 1 = 0$, $x^b - 1 = 0$, $x^c - 1 = 0, \ldots$ sind.

§ 28. Von diesen Grundlagen aus ist der Uebergang zur vollständigen Bestimmung von W für einen beliebigen Werth von n naheliegend. Man zerlege nämlich n in theilerfremde Primzahlen oder Primzahlpotenzen $a, b, c, \ldots$ und setze $r^{\frac{nn}{aa}} = A$, $r^{\frac{nn}{bb}} = B$, $r^{\frac{nn}{cc}} = C, \ldots$: dann werden $A, B, C, \ldots$ primitive Wurzeln der Gleichungen

$$x^a - 1 = 0, \; x^b - 1 = 0, \; x^c - 1 = 0, \ldots,$$

und W wird das Product der Factoren

$$\begin{aligned} &1 + A + A^4 + A^9 + \cdots + A^{(a-1)^2}, \\ &1 + B + B^4 + B^9 + \cdots + B^{(b-1)^2}, \\ &1 + C + C^4 + C^9 + \cdots + C^{(c-1)^2}, \ldots \end{aligned}$$

Nun können diese einzelnen Factoren nach den Resultaten von §§ 20, 21, 23 bestimmt werden, und dadurch ist auch der Werth des Productes bekannt. Es wird nicht ohne Nutzen sein, die Regeln für die Bestimmung jener Factoren hier zu schnellem Ueberblicke zusammenzustellen. Da die Wurzel A gleich $\cos \frac{kn}{a} \cdot \frac{360^\circ}{a} + i \sin \frac{kn}{a} \cdot \frac{360^\circ}{a}$ *) ist, so wird das Aggregat $1 + A + A^4 + A^9 + \ldots + A^{(a-1)^2}$, welches wir mit L bezeichnen, ganz ebenso durch die Zahl $\frac{kn}{a}$ bestimmt, wie in unserer allgemeinen Untersuchung W durch k. Hier sind zwölf Fälle zu unterscheiden.

I. Wenn a eine Primzahl von der Form $4\mu + 1$, etwa $= p$ ist oder die Potenz einer solchen Primzahl mit ungeradem Exponenten, und wenn gleichzeitig $\frac{kn}{a}$ quadratischer Rest von p ist, dann wird $L = +\sqrt{a}$.

II. Wenn für a Gleiches gilt, dagegen $\frac{kn}{a}$ quadratischer Nichtrest von p ist, dann wird $L = -\sqrt{a}$.

III. Wenn a eine Primzahl von der Form $4\mu + 3$ ist, etwa $= p$ oder die Potenz einer solchen Primzahl mit ungeradem

*) [*Gauss* setzt aus Versehen $A = \frac{kn}{a} \cdot \frac{360^\circ}{a}$].

Exponenten, und wenn gleichzeitig $\frac{kn}{a}$ quadratischer Rest von p ist, dann wird $L = + i\sqrt{a}$.

IV. Wenn für a Gleiches gilt wie in III., dagegen $\frac{kn}{a}$ quadratischer Nichtrest von p ist, dann wird $L = - i\sqrt{a}$.

V. Wenn a das Quadrat oder eine höhere Potenz einer ungeraden Primzahl mit geradem Exponenten ist, dann wird $L = +\sqrt{a}$.

VI. Wenn $a = 2$ ist, dann wird $L = 0$.

VII. Wenn $a = 4$ oder eine höhere Potenz von 2 mit geradem Exponenten, und zugleich $\frac{kn}{a}$ von der Form $4\mu + 1$ ist, dann wird $L = (1 + i)\sqrt{a}$.

VIII. Wenn für a Gleiches gilt wie in VII., dagegen $\frac{kn}{a}$ von der Form $4\mu + 3$ ist, dann wird $L = (1 - i)\sqrt{a}$.

IX. Wenn $a = 8$ oder eine höhere Potenz von 2 mit ungeradem Exponenten, und zugleich $\frac{kn}{a}$ von der Form $8\mu + 1$ ist, dann wird $L = (1 + i)\sqrt{a}$.

X. Wenn für a Gleiches gilt wie in IX., dagegen $\frac{kn}{a}$ von der Form $8\mu + 3$ ist, dann wird $L = (-1 + i)\sqrt{a}$.

XI. Wenn für a Gleiches gilt, dagegen $\frac{kn}{a}$ von der Form $8\mu + 5$ ist, dann wird $L = (-1 - i)\sqrt{a}$.

XII. Wenn für a Gleiches gilt, dagegen $\frac{kn}{a}$ von der Form $8\mu + 7$ ist, dann wird $L = (1 - i)\sqrt{a}$*).

§ 30. Eine andere Methode zur allgemeinen Bestimmung der Summe W folgt aus den Resultaten der §§ 22 und 24. Setzen wir $\cos\omega + i\sin\omega = \varrho$ und

* [§ 29, der nur ein numerisches Beispiel enthält, ist fortgelassen worden.]

$$\varrho^{\frac{nn}{aa}} = \alpha\,,\quad \varrho^{\frac{nn}{bb}} = \beta\,,\quad \varrho^{\frac{nn}{cc}} = \gamma\,,\ \ldots$$

so dass $r = \varrho^k$, $A = \alpha^k$, $B = \beta^k$, $C = \gamma^k$, ... ist, dann wird

$$1 + \varrho + \varrho^4 + \varrho^9 + \cdots + \varrho^{(n-1)^2}$$

das Product der Factoren

$$1 + \alpha + \alpha^4 + \alpha^9 + \cdots + \alpha^{(a-1)^2},$$
$$1 + \beta + \beta^4 + \beta^9 + \cdots + \beta^{(b-1)^2},$$
$$1 + \gamma + \gamma^4 + \gamma^9 + \cdots + \gamma^{(c-1)^2}, \ldots$$

und folglich W das Product aus den Factoren

$$w = 1 + \varrho + \varrho^4 + \varrho^9 + \cdots + \varrho^{(n-1)^2},$$

$$\mathfrak{A} = \frac{1 + A + A^4 + A^9 + \cdots + A^{(a-1)^2}}{1 + \alpha + \alpha^4 + \alpha^9 + \cdots + \alpha^{(a-1)^2}},$$

$$\mathfrak{B} = \frac{1 + B + B^4 + B^9 + \cdots + B^{(b-1)^2}}{1 + \beta + \beta^4 + \beta^9 + \cdots + \beta^{(b-1)^2}},$$

$$\mathfrak{C} = \frac{1 + C + C^4 + C^9 + \cdots + C^{(c-1)^2}}{1 + \gamma + \gamma^4 + \gamma^9 + \cdots + \gamma^{(c-1)^2}}, \ldots$$

Hier ist der erste Factor w durch die oben angestellten Untersuchungen (§ 19) bestimmt; die übrigen Factoren $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, ... ergeben sich aus den Formeln der § 22, 24. Um Alles vereint zu haben, stellen wir sie hier nochmals zusammen*). Es sind zwölf Fälle zu unterscheiden, nämlich

I. Wenn a eine (ungerade) Primzahl $= p$ oder die Potenz einer solchen Zahl mit ungeradem Exponenten ist, und zugleich k quadratischer Rest von p, dann wird der entsprechende Factor $\mathfrak{A} = +1$.

II. Wenn für a Gleiches gilt, dagegen k quadratischer Nichtrest von p ist, dann wird $\mathfrak{A} = -1$.

III. Wenn a das Quadrat einer ungeraden Primzahl oder eine höhere Potenz einer solchen mit geradem Exponenten ist, dann wird $\mathfrak{A} = +1$.

*) Offenbar ist das, was dort k und h war, hier $\frac{n}{a}$ und k für den zweiten Factor, $\frac{n}{b}$ und k für den dritten Factor, u. s. w.

IV. Wenn $a = 4$ oder eine höhere Potenz von 2 mit geradem Exponenten ist, und zugleich k von der Form $4\mu + 1$, dann wird $\mathfrak{A} = +1$.

V. Wenn für a Gleiches gilt wie in IV., dagegen k von der Form $4\mu + 3$ ist, und $\frac{n}{a}$ von der Form $4\mu + 1$, dann wird $\mathfrak{A} = -i$.

VI. Wenn für a Gleiches gilt wie in IV., dagegen k von der Form $4\mu + 3$ ist, und $\frac{n}{a}$ von der Form $4\mu + 3$, dann wird $\mathfrak{A} = +i$.

VII. Wenn $a = 8$ oder eine höhere Potenz von 2 mit ungeradem Exponenten ist, und k von der Form $8\mu + 1$, dann wird $\mathfrak{A} = +1$.

VIII. Wenn für a Gleiches gilt wie in VII., dagegen k von der Form $8\mu + 5$ ist, dann wird $\mathfrak{A} = -1$.

IX. Wenn für a Gleiches gilt wie in VII., dagegen k von der Form $8\mu + 3$ ist, und $\frac{n}{a}$ von der Form $4\mu + 1$, dann wird $\mathfrak{A} = +i$.

X. Wenn für a Gleiches gilt wie in VII., dagegen k von der Form $8\mu + 3$ ist, und $\frac{n}{a}$ von der Form $4\mu + 3$, dann wird $\mathfrak{A} = -i$.

XI. Wenn für a Gleiches gilt wie in VII., dagegen k von der Form $8\mu + 7$ ist, und $\frac{n}{a}$ von der Form $4\mu + 1$, dann wird $\mathfrak{A} = -i$.

XII. Wenn für a Gleiches gilt wie in VII., dagegen k von der Form $8\mu + 7$, und $\frac{n}{a}$ von der Form $4\mu + 3$ ist, dann wird $\mathfrak{A} = +i$.

Den Fall $a = 2$ übergehen wir. Hier würde zwar $\mathfrak{A} = \frac{0}{0}$, d. h. unbestimmt erscheinen, aber doch beständig $W = 0$ sein.

Die übrigen Factoren $\mathfrak{B}$, $\mathfrak{C}$, ... hängen ebenso von b, c, ... ab, wie $\mathfrak{A}$ von a, so weit diese Grössen in die Bestimmung jener eingehen *).

---

*) [§ 31 behandelt dasselbe numerische Beispiel wie § 29 nach der zweiten Methode.]

§ 32. Da der Werth von W durch zwei Methoden bestimmt ist, deren eine sich auf die Beziehungen der Zahlen $\frac{nk}{a}, \frac{nk}{b}, \frac{nk}{c}, \ldots$ zu den Zahlen $a, b, c, \ldots$ stützt, während die andere von den Beziehungen des k zu den Zahlen $a, b, c, \ldots$ abhängt, so muss zwischen all diesen Relationen eine gewisse Abhängigkeitsbeziehung bestehen, derart dass eine jede aus den übrigen bestimmbar ist. Wir nehmen an, alle Zahlen $a, b, c, \ldots$ seien Primzahlen, und k sei $= 1$; die Factoren $a, b, c, \ldots$ wollen wir in zwei Classen vertheilen. Die erste möge die Zahlen von der Form $4\mu + 1$ enthalten; diese bezeichnen wir durch $p, p', p'', \ldots$ Die zweite Classe möge aus den Zahlen von der Form $4\mu + 3$ bestehen; diese sollen durch $q, q', q'', \ldots$ ausgedrückt werden. Die Anzahl dieser letzten Zahlen bezeichnen wir durch m. Hierauf bemerken wir zunächst, dass n von der Form $4\mu + 1$ wird, sobald m gerade ist (hierher muss auch der Fall gerechnet werden, dass in der zweiten Classe überhaupt keine Factoren vorkommen, dass also $m = 0$ ist); dass dagegen n von der Form $4\mu + 3$ wird, wenn m ungerade ist. Nun vollzieht sich die Bestimmung von W durch die erste Methode folgendermaassen. Es mögen die Zahlen $P, P', P'', \ldots; Q, Q', Q'', \ldots$ so von den Beziehungen der Zahlen $\frac{n}{p}, \frac{n}{p'}, \frac{n}{p''}, \ldots; \frac{n}{q}, \frac{n}{q'}, \frac{n}{q''}, \ldots$ zu den Zahlen $p, p', p'', \ldots; q, q', q'', \ldots$ abhängen, dass man setzt

$$P = +1, \text{ wenn } \frac{n}{p} \text{ quadratischer Rest von } p \text{ ist,}$$

$$P = -1, \text{ wenn } \frac{n}{p} \text{ quadratischer Nichtrest von } p \text{ ist}$$

u. s. f. für die übrigen Zahlen. Dann wird W das Product der Factoren $P\sqrt{p}, P'\sqrt{p'}, P''\sqrt{p''}, \ldots; iQ\sqrt{q}, iQ'\sqrt{q'}, iQ''\sqrt{q''}, \ldots$ und also

$$W = PP'P'' \ldots QQ'Q'' \ldots i^m \sqrt{n}.$$

Nach der zweiten Methode, oder vielmehr schon nach den Vorschriften des § 19 wird

$W = +\sqrt{n}$, wenn n die Form $4\mu + 1$ hat, d. h. wenn m gerade ist.

$W = +i\sqrt{n}$, wenn n die Form $4\mu + 3$ hat, d. h. wenn m ungerade ist.

Beide Fälle umfasst gleichzeitig die folgende Formel

$$W = i^{m^2} \sqrt{n}.$$

Demnach ist

$$PP'P'' \ldots QQ'Q'' \ldots = i^{m^2 - m}.$$

Nun wird $i^{m^2 - m}$ gleich 1, wenn m von der Form 4μ oder $4\mu + 1$ ist, dagegen $= -1$, wenn m von der Form $4\mu + 2$ oder $4\mu + 3$ ist. Hieraus fliesst der folgende höchst elegante Satz.

Lehrsatz. Bezeichnen $a, b, c, \ldots$ ungleiche, ungerade, positive Primzahlen, deren Product $= n$ ist, und unter denen m von der Form $4\mu + 3$ sind, während die übrigen die Form $4\mu + 1$ haben, dann wird die Anzahl derjenigen Zahlen $a, b, c, \ldots$, für die bezw. $\frac{n}{a}, \frac{n}{b}, \frac{n}{c}, \ldots$ Nichtreste sind, gerade werden, wenn m von der Form 4μ oder $4\mu + 1$ ist, ungerade dagegen, wenn m von der Form $4\mu + 2$ oder $4\mu + 3$ ist.

Ist z. B. $a = 3$, $b = 5$, $c = 7$, $d = 11$, so haben wir drei Zahlen von der Form $4\mu + 3$, nämlich 3, 7, 11; und es ist $5.7.11\,R\,3$; $3.7.11\,R\,5$; $3.5.11\,R\,7$; $3.5.7\,N\,11$ d. h. allein $\frac{n}{d}$ ist Nichtrest von d.

§ 33. Das berühmte Fundamentaltheorem über die quadratischen Reste ist nichts anderes als ein besonderer Fall des eben entwickelten Satzes. Beschränken wir nämlich die Anzahl der Zahlen $a, b, c, \ldots$ auf zwei, so ist klar, dass, wenn nur eine derselben oder keine von der Form $4\mu + 3$ ist, dann zugleich aRb, bRa oder zugleich aNb, bNa sein muss; wenn dagegen beide von der Form $4\mu + 3$ sind, muss die eine Nichtrest der anderen, und diese Rest der ersten sein. So haben wir also einen vierten Beweis dieses wichtigen Satzes, für den wir einen ersten und zweiten Beweis in den »Disquisitiones arithmeticae« und neulich einen dritten in einer besonderen Abhandlung (Comment. Gott. T. XVI) gegeben haben; zwei andere, die sich wieder auf völlig verschiedene Grundlagen aufbauen, werden wir später darlegen. Es ist sehr merkwürdig, dass dieser so schöne Satz, der zuerst recht hartnäckig allen Beweisversuchen widerstand, so viel später auf so zahlreichen weit verschiedenen Wegen erreicht werden konnte.

§ 34. Auch die übrigen Sätze, welche gleichsam eine Ergänzung des Fundamentaltheorems ausmachen, und die sich auf die Bestimmung derjenigen Primzahlen beziehen, deren Reste oder Nichtreste -1, $+2$, -2 sind, können aus denselben Principien hergeleitet werden. Wir beginnen mit dem Reste $+2$.

Wir setzen $n = 8a$ und verstehen unter a eine Primzahl; k sei $= 1$. Nach der Methode des § 28 wird W das Product aus zwei Factoren, deren einer $+\sqrt{a}$ oder $+i\sqrt{a}$ ist, falls 8 oder, was dasselbe besagt, 2 quadratischer Rest von a ist; dagegen $-\sqrt{a}$ oder $-i\sqrt{a}$, falls 2 quadratischer Nichtrest von a ist. Der zweite Factor hingegen ist

$$(1+i)\sqrt{8}, \text{ wenn } a \text{ die Form } 8\mu+1 \text{ hat,}$$
$$(-1+i)\sqrt{8}, \text{ wenn } a \text{ die Form } 8\mu+3 \text{ hat,}$$
$$(-1-i)\sqrt{8}, \text{ wenn } a \text{ die Form } 8\mu+5 \text{ hat,}$$
$$(1-i)\sqrt{8}, \text{ wenn } a \text{ die Form } 8\mu+7 \text{ hat.}$$

Nun wird nach § 18 stets $W = (1+i)\sqrt{n}$. Dividirt man dies durch die vier Werthe des zweiten Factors, so nimmt offenbar der erste Factor die Gestalt an

$$+\sqrt{a}, \text{ wenn } a \text{ die Form } 8\mu+1 \text{ hat,}$$
$$-i\sqrt{a}, \text{ wenn } a \text{ die Form } 8\mu+3 \text{ hat,}$$
$$-\sqrt{a}, \text{ wenn } a \text{ die Form } 8\mu+5 \text{ hat,}$$
$$+i\sqrt{a}, \text{ wenn } a \text{ die Form } 8\mu+7 \text{ hat.}$$

Hieraus folgt sofort, dass im ersten und im vierten Falle 2 Rest von a, im zweiten und im dritten dagegen 2 Nichtrest von a ist.

§ 35. Die Primzahlen, deren Rest oder Nichtrest -1 ist, lassen sich leicht mit Hülfe des folgenden Satzes feststellen, der auch an und für sich bemerkenswerth ist.

Lehrsatz. Das Product aus den beiden Factoren

$$W' = 1 + r^{-1} + r^{-4} + \cdots + r^{-(n-1)^2},$$
$$W = 1 + r + r^4 + \cdots + r^{(n-1)^2}$$

ist $= n$, wenn n ungerade ist; dagegen $= 0$, wenn n ungerade mal gerade ist, und endlich $= 2n$, wenn n gerade mal gerade ist.

Beweis. Da offenbar

$$\begin{aligned} W &= r + r^4 + r^9 + \cdots + r^{n^2} \\ &= r^4 + r^9 + r^{16} + \cdots + r^{(n+1)^2} \\ &= r^9 + r^{16} + \cdots + r^{(n+2)^2} = \cdots, \end{aligned}$$

so kann das Product WW' folgendermaassen geschrieben werden

$$\begin{aligned} & 1 + r + r^4 + r^9 + \cdots + r^{(n-1)^2} \\ & + r^{-1}(r + r^4 + r^9 + r^{16} + \cdots + r^{n^2}) \\ & + r^{-4}(r^4 + r^9 + r^{16} + r^{25} + \cdots + r^{(n+1)^2}) \\ & + r^{-9}(r^9 + r^{16} + r^{25} + r^{36} + \cdots + r^{(n+2)^2}) \\ & + \cdots\cdots\cdots\cdots\cdots\cdots \\ & + r^{-(n-1)^2}(r^{(n-1)^2} + r^{n^2} + r^{(n+1)^2} + \cdots + r^{(2n-2)^2}); \end{aligned}$$

addirt man dieses Aggregat spaltenweise, dann ergiebt sich

$$\begin{aligned} & n \\ & + r(1 + r^2 + r^4 + r^6 + \cdots + r^{2n-2}) \\ & + r^4(1 + r^4 + r^8 + r^{12} + \cdots + r^{4n-4}) \\ & + r^9(1 + r^6 + r^{12} + r^{18} + \cdots + r^{6n-6}) \\ & + \cdots\cdots\cdots\cdots\cdots\cdots \\ & + r^{(n-1)^2}(1 + r^{2n-2} + r^{4n-4} + r^{6n-6} + \cdots + r^{2(n-1)^2}). \end{aligned}$$

Ist nun n ungerade, dann verschwinden die einzelnen Glieder dieser Summe ausser dem ersten, n; denn offenbar wird das zweite $r\dfrac{r^{2n}-1}{r^2-1}$, das dritte $r^4\dfrac{r^{4n}-1}{r^4-1}$, ... Falls aber n gerade ist, muss man ausser dem ersten noch das Glied

$$r^{\frac{1}{4}n^2}(1 + r^n + r^{2n} + r^{3n} + \cdots + r^{n^2-n})$$

absondern, welches $= n r^{\frac{1}{4}n^2}$ wird. Im ersten Falle ist also $WW' = n$; im zweiten $= n + n r^{\frac{1}{4}n^2}$. Nun wird $r^{\frac{1}{4}n^2} = +1$, wenn n gerade mal gerade ist; dabei erhält man also

$$WW' = 2n.$$

Dagegen wird $r^{\frac{1}{4}n^2} = -1$, wenn n ungerade mal gerade ist; daraus geht $WW' = 0$ hervor. W. z. b. w.

§ 36. Aus § 22 ist es bekannt, dass, wenn n eine ungerade Primzahl ist, $\dfrac{W'}{W} = +1$ oder $= -1$ wird, je nachdem -1 Rest oder Nichtrest von n ist. Folglich muss im

ersten Falle $W'^2 = +n$ und im zweiten $W'^2 = -n$ sein; und deshalb schliessen wir aus § 13, dass der erste Fall nur dann statthaben kann, wenn n von der Form $4\mu + 1$ ist; der zweite nur dann, wenn n von der Form $4\mu + 3$ ist.

Endlich folgt aus der Combination der Bedingungen für die Reste $+2$ und -1 von selbst, dass -2 Rest jeder Primzahl von der Form $8\mu + 1$ oder $8\mu + 3$ und Nichtrest jeder Primzahl von der Form $8\mu + 5$ oder $8\mu + 7$ wird.



[Fünfter und Sechster] Beweis des Fundamentaltheorems der quadratischen Reste.

Veröffentlicht in den

Commentationes societatis regiae scientiarum Gottingensis recentiores.

Vol. IV; Gottingae 1818.

(Werke, Band II. p. 47—64.)

Das Fundamentaltheorem über die quadratischen Reste, welches zu den schönsten Wahrheiten der höheren Arithmetik zu rechnen ist, wurde durch Induction leicht entdeckt, allein sein Beweis war ausserordentlich schwierig. In diesem Zweige der Mathematik geschieht es häufig, dass sich dem Forscher einfache Wahrheiten durch Induction von selbst aufdrängen, dass aber ihre Beweise sehr tief versteckt sind und erst nach vielen vergeblichen Versuchen, auf einem ganz anderen Wege als man sie vermuthete, ans Licht gezogen werden können. Ferner geschieht es nicht selten, dass, wenn erst ein Weg aufgefunden ist, sich dann mehrere öffnen, die zu demselben Ziele führen; einige kürzer und directer, andere gewissermaassen von der Seite her und aus so verschiedenen Principien entspringend, dass man kaum eine Verbindung zwischen ihnen und der vorgelegten Frage vermuthet haben würde. Dieser merkwürdige Zusammenhang zwischen versteckten Wahrheiten leiht solchen Betrachtungen nicht nur einen eigenthümlichen Reiz, sondern verdient auch deshalb eifrig durchforscht und ergründet zu werden, weil aus ihm nicht selten neue Hülfsmittel oder Bereicherungen der Wissenschaft selbst fliessen.

Obwohl daher das arithmetische Theorem, um das es sich hier handelt, durch voraufgehende Bemühungen mit vier unter einander völlig verschiedenen Beweisen versehen ist*), und

*) Zwei sind in den Disquisitiones arithmeticae, Abschn. IV und V. auseinandergesetzt; der dritte in einer besonderen Abhandlung

so für völlig erledigt angesehen werden kann, so kehre ich dennoch zu demselben Gegenstande zurück und füge noch zwei andere Beweise hinzu, welche sicher auf diese Frage ein neues Licht werfen werden. Der erste derselben ist dem früheren dritten einigermaassen verwandt, indem er von demselben Hülfssatze ausgeht; dann aber verfolgt er einen verschiedenen Weg, so dass er mit Recht als neuer Beweis gelten kann, welcher an Kürze jenem dritten wenn nicht überlegen, so doch mindestens nicht untergeordnet ist. Der sechste Beweis dagegen stützt sich auf ein völlig verschiedenes, versteckteres Princip und liefert ein neues Beispiel des merkwürdigen Zusammenhanges zwischen arithmetischen Wahrheiten, die beim ersten Anblicke sehr weit von einander entfernt zu sein scheinen*).

Fünfter Beweis des Fundamentaltheorems in der Theorie der quadratischen Reste.

§ 1. Wir haben bereits in der Einleitung angekündigt, dass der fünfte und der dritte Beweis von demselben Hülfssatze ausgehen. Der Bequemlichkeit halber scheint es angezeigt, ihn an diesem Orte in Bezeichnungen zu wiederholen, welche der vorliegenden Untersuchung angepasst sind.

Hülfssatz. Es sei m eine positive ungerade Primzahl, M eine ganze durch m nicht theilbare Zahl; wir nehmen die kleinsten positiven Reste der Zahlen

$$M, 2M, 3M, 4M, \ldots \tfrac{1}{2}(m-1)M$$

modulo m, welche theils kleiner sind als $\frac{1}{2}m$ theils grösser; die Anzahl der letzten sei $= n$. Dann wird M quadratischer Rest oder Nichtrest von m, je nachdem n gerade oder ungerade ist.

Beweis. Wir bezeichnen die Reste, welche kleiner sind als $\frac{1}{2}m$, mit $a, b, c, d, \ldots$ und die übrigen, welche grösser sind als $\frac{1}{2}m$, mit $a', b', c', d', \ldots$. Die Ergänzungen der letzten zu m, nämlich $m - a', m - b', m - c', m - d', \ldots$ werden offenbar sämmtlich kleiner als $\frac{1}{2}m$ und sind sowohl unter sich

Comment. Soc. Gotting. Vol. XVI; der vierte ist in die Abhandlung »Summatio quarundam serierum singularium« Comment. Recentiores, Vol. I eingeflochten.

*) [Die weiteren Ausführungen der Einleitung sind unterdrückt, da sie sich nicht auf unseren besonderen Gegenstand beziehen.]

als von den Resten $a, b, c, d, \ldots$ verschieden. Deshalb werden sie, mit diesen zusammengenommen, abgesehen von der Ordnung, mit allen Zahlen $1, 2, 3, 4, \ldots, \frac{1}{2}(m-1)$ identisch. Setzt man daher das Product

$$1 \cdot 2 \cdot 3 \cdot 4 \ldots \frac{1}{2}(m-1) = P,$$

so wird

$$P = abcd \ldots \times (m-a')(m-b')(m-c')(m-d') \ldots,$$

und also

$$(-1)^n P = abcd \ldots \times (a'-m)(b'-m)(c'-m)(d'-m) \ldots$$

Ferner wird modulo m

$$PM^{\frac{1}{2}(m-1)} \equiv abcd \ldots \times a'b'c'd' \ldots$$
$$\equiv abcd \ldots (a'-m)(b'-m)(c'-m)(d'-m) \ldots$$

und daher

$$PM^{\frac{1}{2}(m-1)} \equiv P(-1)^n.$$

Hieraus folgt $M^{\frac{1}{2}(m-1)} \equiv \pm 1$, wo das obere oder das untere Zeichen gilt, je nachdem n gerade oder ungerade ist. Mit Hülfe des Satzes § 106 der Disquisitiones arithmeticae (siehe S. 11) ergiebt sich dann von selbst der Hülfssatz.

§ 2. Lehrsatz. Es seien m und M ganze, positive, ungerade, theilerfremde Zahlen und n die Anzahl derjenigen kleinsten positiven Reste von

$$M, 2M, 3M, \ldots \frac{1}{2}(m-1)M$$

modulo m, welche $\frac{1}{2}m$ übertreffen; ebenso sei N die Anzahl derjenigen kleinsten positiven Reste von

$$m, 2m, 3m, \ldots \frac{1}{2}(M-1)m$$

modulo M, welche $\frac{1}{2}M$ übertreffen. Dann sind die drei Zahlen n, N, $\frac{1}{4}(m-1)(M-1)$ entweder sämmtlich gerade oder eine unter ihnen gerade und die beiden anderen ungerade.

Beweis. Wir bezeichnen mit

f den Complex der Zahlen $1, 2, 3, \ldots \frac{1}{2}(m-1)$,
f' den Complex der Zahlen $m-1, m-2, m-3, \ldots \frac{1}{2}(m+1)$,
F den Complex der Zahlen $1, 2, 3, \ldots \frac{1}{2}(M-1)$,
F' den Complex der Zahlen $M-1, M-2, M-3, \ldots \frac{1}{2}(M+1)$.

Dann zeigt also n an, wieviel Zahlen Mf ihre, modulo m genommenen kleinsten positiven Reste im Complexe f' haben;

ebenso zeigt N an, wieviel Zahlen mF ihre, modulo M genommenen kleinsten positiven Reste im Complexe F' haben. Endlich bezeichnen wir durch

φ den Complex der Zahlen $1, 2, 3, \ldots \frac{1}{2}(mM-1)$
φ' den Complex der Zahlen

$$mM-1,\ mM-2,\ mM-3, \ldots \tfrac{1}{2}(mM+1).$$

Da jede durch m nicht theilbare Zahl, modulo m genommen, einem der Reste in f oder einem derjenigen in f' congruent sein muss; und da genau so jede durch M nicht theilbare ganze Zahl, modulo M genommen, einem der Reste in F oder einem derjenigen in F' congruent sein muss, so werden alle Zahlen φ, unter denen offenbar keine gleichzeitig durch m und durch M theilbar ist, sich auf folgende Art in acht Classen vertheilen lassen:

I. Zur ersten Classe rechnen wir diejenigen Zahlen, welche modulo m einer Zahl aus f und modulo M genommen einer Zahl aus F congruent sind. Die Anzahl dieser Zahlen bezeichnen wir mit α.

II. Die Zahlen, welche modd. m, M bezw. zu Zahlen aus f, F' congruent sind. Die Anzahl dieser Zahlen setzen wir $= \beta$.

III. Die Zahlen, welche modd. m, M bezw. zu Zahlen aus f', F congruent sind, ihre Anzahl sei $= \gamma$.

IV. Die Zahlen, welche modd. m, M bezw. zu Zahlen aus f', F' congruent sind; ihre Anzahl sei $= \delta$.

V. Durch m theilbare Zahlen, welche mod. M zu Resten aus F congruent sind.

VI. Durch m theilbare Zahlen, welche modulo M zu Resten aus F' congruent sind.

VII. Durch M theilbare Zahlen, welche modulo m zu Resten aus f congruent sind.

VIII. Durch M theilbare Zahlen, welche modulo m zu Resten aus f' congruent ist.

Offenbar umfassen die Classen V und VI zusammen genommen alle Zahlen mF; die Anzahl der in VI enthaltenen ist $= N$, und also die Anzahl der in V enthaltenen

$$\tfrac{1}{2}(M-1)-N.$$

Ebenso umfassen die Classen VII und VIII zusammen genommen alle Zahlen Mf; in VII giebt es n Zahlen, und also in VIII

$$\tfrac{1}{2}(m-1)-n.$$

Auf ähnliche Weise können alle Zahlen g' in acht Classen IX, ... XVI vertheilt werden. Behält man dafür dieselbe Anordnung bei, so erkennt man leicht, dass die in den Classen

IX, X, XI, XII, XIII, XIV, XV, XVI

enthaltenen Zahlen bezw. die Complemente der Zahlen in den Classen

IV, III, II, I, VI, V, VIII, VII

zu mM sind, so dass es also δ Zahlen in der Classe IX giebt, γ in der Classe X u. s. f. Nun ist es klar, dass, wenn alle Zahlen der ersten mit allen Zahlen der neunten Classe vereinigt werden, dann alle Zahlen unterhalb mM sich ergeben, welche modulo m einer Zahl aus f und modulo M einer Zahl aus F congruent sind. Ferner erkennt man leicht, dass ihre Anzahl gleich der Anzahl aller Combinationen der einzelnen f mit den einzelnen F sind. Wir haben also

$$\alpha + \delta = \tfrac{1}{4}(m-1)(M-1);$$

und auf ähnliche Art erhält man

$$\beta + \gamma = \tfrac{1}{4}(m-1)(M-1).$$

Vereinigt man alle Zahlen der Classen II, IV, VI, so hat man offenbar alle Zahlen unterhalb $\frac{1}{2}mM$, welche einem der Reste aus F' modulo M congruent sind. Dieselben Zahlen können nun auch so dargestellt werden

$$F',\ M + F',\ 2M + F',\ 3M + F',\ \ldots\ \tfrac{1}{2}(m-3)M + F';$$

folglich wird die Gesammtanzahl $= \frac{1}{4}(m-1)(M-1)$, d. h. wir erhalten

$$\beta + \delta + N = \tfrac{1}{4}(m-1)(M-1).$$

Auf gleiche Weise folgt durch die Vereinigung aller Classen III, IV, VIII,

$$\gamma + \delta + n = \tfrac{1}{4}(m-1)(M-1).$$

Aus diesen vier Gleichungen entspringen die folgenden

$$\begin{aligned} 2\alpha &= \tfrac{1}{4}(m-1)(M-1) + n + N, \\ 2\beta &= \tfrac{1}{4}(m-1)(M-1) + n - N, \\ 2\gamma &= \tfrac{1}{4}(m-1)(M-1) - n + N, \\ 2\delta &= \tfrac{1}{4}(m-1)(M-1) - n - N. \end{aligned}$$

Jede dieser Gleichungen zeigt die Richtigkeit des aufgestellten Theorems.

§ 3. Setzen wir nun voraus, m und M seien Primzahlen, dann folgt aus der Combination des vorhergehenden Lehrsatzes mit dem Hülfssatze aus § 1 sogleich das Fundamentaltheorem. Denn es ergiebt sich:

I. Sind beide Zahlen m und M oder ist wenigstens eine derselben von der Form $4k+1$, dann wird die Zahl

$$\tfrac{1}{4}(m-1)(M-1)$$

gerade; also werden n und N entweder gleichzeitig gerade oder gleichzeitig ungerade; und deswegen ist entweder jede der beiden Zahlen m und M quadratischer Rest der anderen, oder jede ist quadratischer Nichtrest der anderen.

II. Wenn beide Zahlen m und M von der Form $4k+3$ sind, dann wird $\frac{1}{4}(m-1)(M-1)$ ungerade, und somit eine der Zahlen n und N gerade und die andere ungerade. Deswegen ist die eine der Zahlen m und M quadratischer Rest der andern, während diese quadratischer Nichtrest der ersten ist. W. z. b. w.

Sechster Beweis des Fundamentaltheorems in der Theorie der quadratischen Reste. [12]

§ 1. Lehrsatz. Bezeichnet p eine (positive, ungerade) Primzahl, n eine ganze positive durch p nicht theilbare Zahl und x eine unbestimmte Grösse, dann wird die Function

$$1 + x^n + x^{2n} + x^{3n} + \ldots + x^{np-n}$$

durch

$$1 + x + x^2 + x^3 + \ldots + x^{p-1}$$

theilbar werden.

Beweis. Wir nehmen eine ganze positive Zahl g an, für welche $gn \equiv 1 \pmod{p}$ wird, und setzen $gn = 1 + hp$. Dann wird

$$\frac{1 + x^n + x^{2n} + x^{3n} + \ldots + x^{np-n}}{1 + x + x^2 + x^3 + \ldots + x^{p-1}} = \frac{(1-x^{np})(1-x)}{(1-x^n)(1-x^p)}$$

$$= \frac{(1-x^{np})(1-x^{gn}-x+x^{hp+1})}{(1-x^n)(1-x^p)}$$

$$= \frac{1-x^{np}}{1-x^p}\cdot\frac{1-x^{gn}}{1-x^n} - \frac{x(1-x^{np})}{1-x^n}\cdot\frac{1-x^{hp}}{1-x^p}$$

und somit offenbar eine ganze Function. W. z. b. w.

Jede ganze Function von x, welche durch $\frac{1-x^{np}}{1-x^n}$ theilbar ist, wird demnach auch durch $\frac{1-x^p}{1-x}$ theilbar sein.

§ 2. a möge eine primitive positive Wurzel für den Modul p bezeichnen, d. h. a soll eine derartige positive ganze Zahl sein, dass die kleinsten positiven Reste der Potenzen 1, $a, a^2, a^3, \ldots a^{p-2}$ nach dem Modul p genommen, ohne Rücksicht auf die Ordnung, mit den Zahlen $1, 2, 3, 4, \ldots p-1$ identisch werden. Bezeichnet man ferner durch $f(x)$ die Function

$$x + x^a + x^{a^2} + x^{a^3} + \ldots + x^{a^{p-2}} + 1,$$

dann ist es klar, dass $f(x) - 1 - x - x^2 - x^3 - \cdots - x^{p-1}$ durch $1 - x^p$ theilbar wird, und also um so mehr durch $\frac{1-x^p}{1-x} = 1 + x + x^2 + x^3 + \cdots + x^{p-1}$; folglich wird $f(x)$ selbst durch dieses $\frac{1-x^p}{1-x}$ theilbar. Da nun x eine unbestimmte Grösse bezeichnet, so wird auch $f(x^n)$ durch $\frac{1-x^{np}}{1-x^n}$ theilbar, und deshalb (§ 1) auch durch $\frac{1-x^p}{1-x}$, sobald n eine ganze, durch p nicht theilbare Zahl ist. Wenn hingegen n eine ganze durch p theilbare Zahl ist, dann werden die einzelnen Summanden von $f(x^n)$, je um eine Einheit vermindert, durch $1 - x^p$ theilbar; folglich ist in diesem Falle auch $f(x^n) - p$ durch $1 - x^p$ und folglich auch durch $\frac{1-x^p}{1-x}$ theilbar.

§ 3. **Lehrsatz.** Setzt man

$$x - x^a + x^{a^2} - x^{a^3} + x^{a^4} - \ldots - x^{a^{p-2}} = \xi,$$

dann wird $\xi^2 \mp p$ durch $\frac{1-x^p}{1-x}$ theilbar, wenn man das obere Zeichen nimmt, sobald p von der Form $4k+1$ ist, das untere dagegen, sobald p von der Form $4k+3$ ist.

Beweis. Man sieht leicht ein, dass unter den $(p-1)$ Functionen

$$\begin{aligned}
&+x\,\xi - x^2 + x^{a+1} - x^{a^2+1} + \cdots + x^{a^{p-2}+1},\\
&-x^{a}\,\xi - x^{2a} + x^{a^2+a} - x^{a^3+a} + \cdots + x^{a^{p-1}+a},\\
&+x^{a^2}\,\xi - x^{2a^2} + x^{a^3+a^2} - x^{a^4+a^2} + \cdots + x^{a^{p}+a^2},\\
&-x^{a^3}\,\xi - x^{2a^3} + x^{a^4+a^3} - x^{a^5+a^3} + \cdots + x^{a^{p+1}+a^3},\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
&-x^{a^{p-2}}\,\xi - x^{2a^{p-2}} + x^{a^{p-1}+a^{p-2}} - x^{a^{p}+a^{p-2}} + \cdots\\
&\qquad\qquad + x^{a^{2p-4}+a^{p-2}}
\end{aligned}$$

die erste $= 0$ wird, und dass die anderen einzeln durch $1 - x^p$ theilbar werden. Daher ist auch die Gesammtsumme durch $1 - x^p$ theilbar; diese Summe ist

$$\begin{aligned}
&= \xi^2 - (f(x^2) - 1) + (f(x^{a+1}) - 1) - (f(x^{a^2+1}) - 1)\\
&\qquad + (f(x^{a^3+1}) - 1) - \cdots + (f(x^{a^{p-2}+1}) - 1)\\
&= \xi^2 - f(x^2) + f(x^{a+1}) - f(x^{a^2+1}) + f(x^{a^3+1}) - \cdots\\
&\qquad + f(x^{a^{p-2}+1}) = \Omega.
\end{aligned}$$

Dieser Ausdruck Ω ist also gleichfalls durch $\frac{1-x^p}{1-x}$ theilbar. Nun ist unter den Exponenten 2, $a+1$, a^2+1, $a^3+1, \ldots a^{p-2}+1$ nur ein einziger durch p theilbar, nämlich $a^{\frac{1}{2}(p-1)}+1$; folglich werden nach dem vorhergehenden Paragraphen die einzelnen Theile von Ω, nämlich

$$f(x^2),\ f(x^{a+1}),\ f(x^{a^2+1}),\ f(x^{a^3+1}), \ldots$$

mit Ausnahme des einen Gliedes $f(x^{a^{\frac{1}{2}(p-1)}+1})$ durch $\frac{1-x^p}{1-x}$ theilbar. Lässt man jene Glieder fort, so erkennt man, dass die durch $\frac{1-x^p}{1-x}$ theilbare Function zurückbleibt:

$$\xi^2 \mp f(x^{a^{\frac{1}{2}(p-1)}+1}),$$

wobei das obere oder das untere Zeichen gilt, je nachdem p die Form $4k+1$ oder $4k+3$ hat. Da überdies

$$f(x^{a^{\frac{1}{2}(p-1)}+1}) - p$$

durch $\frac{1-x^p}{1-x}$ theilbar ist, so wird auch $\xi^2 \mp p$ durch $\frac{1-x^p}{1-x}$ theilbar; w. z. b. w.

Damit das doppelte Vorzeichen keine Schwierigkeit entstehen lässt, wollen wir durch ε die Zahl $+1$ oder -1 bezeichnen, je nachdem p von der Form $4k+1$ oder $4k+3$ ist. Demnach wird $\dfrac{(1-x)(\xi^2-\varepsilon p)}{1-x^p}$ eine ganze Function von x. Wir wollen sie durch Z bezeichnen.

§ 4. Nun möge q eine positive ungerade Zahl und also $\frac{1}{2}(q-1)$ eine ganze Zahl sein. Dann wird

$$(\xi\xi)^{\frac{1}{2}(q-1)} - (\varepsilon p)^{\frac{1}{2}(q-1)}$$

durch $\xi^2 - \varepsilon p$ und also auch durch $\dfrac{1-x^p}{1-x}$ theilbar. Setzen wir $\varepsilon^{\frac{1}{2}(q-1)} = \delta$ und

$$\xi^{q-1} - \delta p^{\frac{1}{2}(q-1)} = \frac{1-x^p}{1-x} \cdot Y,$$

so wird Y eine ganze Function von x; und es wird $\delta = +1$, sobald eine der Zahlen p, q oder auch beide die Form $4k+1$ haben; dagegen wird $\delta = -1$, sobald beide Zahlen p q die Form $4k+3$ haben.

§ 5. Jetzt möge q gleichfalls eine (von p verschiedene) Primzahl sein. Nach dem in § 51 der »Disquisitiones arithmeticae« bewiesenen Satze*) ist es klar, dass

$$\xi^q - (x^q - x^{q\alpha} + x^{q\alpha^2} - x^{q\alpha^3} + \cdots - x^{q\alpha^{p-2}})$$

durch q theilbar, d. h. von der Form qX sein wird, wo X eine ganze Function von x ist, auch hinsichtlich der numerischen Coefficienten; (das Gleiche ist auch bei den übrigen, hier in Betracht kommenden ganzen Functionen Z, Y, W zu bemerken). Nun bezeichnen wir für den Modul p und die primitive Wurzel α den Index der Zahl q durch μ, d. h. wir setzen $q \equiv \alpha^\mu$ (mod. p). Dann werden die Zahlen $q, q\alpha, q\alpha^2, q\alpha^3, \ldots q\alpha^{p-2}$ modulo p bezw. den Zahlen $\alpha^\mu, \alpha^{\mu+1}, \alpha^{\mu+2}, \ldots \alpha^{p-2}, 1, \alpha, \alpha^2, \ldots \alpha^{\mu-1}$ congruent, und also

$$x^q - x^{\alpha^\mu},\ x^{q\alpha} - x^{\alpha^{\mu+1}},\ x^{q\alpha^2} - x^{\alpha^{\mu+2}},\ x^{q\alpha^3} - x^{\alpha^{\mu+3}}, \ldots$$
$$\ldots,\ x^{q\alpha^{p-\mu-2}} - x^{\alpha^{p-2}},\ x^{q\alpha^{p-\mu-1}} - x^1,\ x^{q\alpha^{p-\mu}} - x^\alpha,$$
$$x^{q\alpha^{p-\mu+1}} - x^{\alpha^2}, \ldots x^{q\alpha^{p-2}} - x^{\alpha^{\mu-1}}$$

---

* Es ist dies der aus dem *Fermat*schen Theorem folgende Satz, dass die q-te Potenz eines Polynoms $a+b+c+\ldots$ dem Ausdrucke $a^q+b^q+c^q+\ldots$ modulo q congruent wird, sobald q eine Primzahl ist.]

durch $1-x^p$ theilbar. Nimmt man diese Grössen abwechselnd positiv und negativ und summirt sie dann, so wird durch $1-x^p$ theilbar auch die Function

$$x^q - x^{qa} + x^{qa^2} - x^{qa^3} + \cdots - x^{qa^{p-2}} \mp \xi,$$

wobei das obere oder das untere Zeichen gilt, je nachdem μ gerade oder ungerade ist, d. h. je nachdem q quadratischer Rest von p wird oder quadratischer Nichtrest. Wir können also setzen

$$x^q - x^{qa} + x^{qa^2} - x^{qa^3} + \cdots - x^{qa^{p-2}} - \gamma\xi = (1-x^p)W,$$

indem wir $\gamma = +1$ oder $\gamma = -1$ nehmen, je nachdem q quadratischer Rest oder Nichtrest von p ist. Dabei wird W offenbar eine ganze Function.

§ 6. Nach diesen Vorbereitungen folgern wir aus der Combination der vorangehenden Gleichungen

$$q\xi X = \varepsilon p(\delta p^{\frac{1}{2}(q-1)} - \gamma)$$
$$+ \frac{1-x^p}{1-x} \cdot (Z(\delta p^{\frac{1}{2}(q-1)} - \gamma) + Y\xi^2 - W\xi(1-x^q)).$$

Dividiren wir ξX durch

$$x^{p-1} + x^{p-2} + x^{p-3} + \cdots + x + 1,$$

so möge sich der Quotient U und der Rest T ergeben, d. h. es möge

$$\xi X = \frac{1-x^p}{1-x} \cdot U + T$$

sein, wo U, T auch mit Hinblick auf die numerischen Coefficienten ganze Functionen sind, und zwar T von niederer Ordnung als der Divisor. Daher wird

$$qT - \varepsilon p(\delta p^{\frac{1}{2}(q-1)} - \gamma)$$
$$= \frac{1-x^p}{1-x}(Z(\delta p^{\frac{1}{2}(q-1)} - \gamma) + Y\xi^2 - W\xi(1-x^q) - qU).$$

Diese Gleichung kann offenbar nur bestehen, wenn die Glieder auf der linken sowie die auf der rechten Seite für sich verschwinden. Daher wird $\varepsilon p(\delta p^{\frac{1}{2}(q-1)} - \gamma)$ durch q theilbar, und ebenso auch $\delta p^{\frac{1}{2}(q-1)} - \gamma$; demnach wird wegen $\delta^2 = 1$ die Zahl $p^{\frac{1}{2}(q-1)} - \gamma\delta$ durch q theilbar.

Wird nun durch β die positive oder die negative Einheit bezeichnet, je nachdem p quadratischer Rest oder Nichtrest von q ist, dann wird $p^{\frac{1}{2}(q-1)} - \beta$ durch q theilbar, und also auch $\beta - \gamma\delta$. Dies ist unmöglich, wenn nicht $\beta = \gamma\delta$ wird. Hieraus folgt von selbst das Fundamentaltheorem: nämlich

I. so oft entweder beide Zahlen p, q auch oder nur eine die Form $4k + 1$ haben, und also $\delta = +1$ ist, wird $\beta = \gamma$, und so ist dann zugleich q quadratischer Rest von p und p quadratischer Rest von q, oder es ist zugleich q Nichtrest von p und p Nichtrest von q.

II. so oft beide Zahlen p, q die Form $4k + 3$ haben, und also $\delta = -1$ ist, wird $\beta = -\gamma$, und also entweder zugleich q quadratischer Rest von p und p Nichtrest von q, oder zugleich q Nichtrest von p und p Rest von q. W. z. b. w.

Anmerkungen und Erläuterungen*).

Ueber die Wichtigkeit und die Tragweite des von *C. Fr. Gauss* als Fundamentaltheorem bezeichneten Satzes spricht sich *E. Kummer***) folgendermaassen aus: »Die Reciprocitätsgesetze, welche unter den Resten und Nichtresten der Potenzen statt haben, bilden gewissermaassen den Schlussstein der Lehre von den Potenzresten und eröffnen zugleich den Weg für weitere und tiefer liegende arithmetische Untersuchungen. Sie sind in diesen beiden Beziehungen für die Zahlentheorie von grosser Wichtigkeit; aber eine noch höhere Bedeutung haben sie in der geschichtlichen Entwickelung dieser mathematischen Disciplin dadurch erlangt, dass die Beweise derselben, so weit sie überhaupt gefunden sind, fast gänzlich aus neuen, bis dahin noch unerforschten Gebieten haben geschöpft werden müssen, welche so der Wissenschaft aufgeschlossen sind.

Diese Worte rechtfertigen wohl hinreichend das Unternehmen, die von *Gauss* gegebenen, auf quadratische Reste und Nichtreste bezüglichen Beweise in deutscher Uebersetzung zusammenzustellen, zumal da in diesen Untersuchungen fast alle Wege aufgedeckt sind, auf denen es bisher gelungen ist, zum Reciprocitätsgesetze durchzudringen.

Hinweisen müssen wir hier ausdrücklich auf die sehr verdienstvolle und interessante Monographie von *Oswald Baumgart*: »Ueber das quadratische Reciprocitätsgesetz. Eine vergleichende Darstellung der Beweise ... und der denselben zu Grunde liegenden Principien«, Inaug. Diss. Gött. 1885. In dieser Schrift werden die *Gauss*'schen Beweise, wie natürlich, gleichfalls behandelt, allein mit alle den im Laufe der Zeit aufgefundenen Vereinfachungen, während hier gerade auf die Originaldarstellung das Hauptgewicht gelegt ist. Der Vereinfachungen,

---

* Die im vorausgehenden Texte in eckige Klammern eingeschlossenen kurzen Bemerkungen sind als Erläuterungen vom Herausgeber beigefügt worden.

** Abhandl. d. Berl. Akad. (1859) p. 19.

welche wir späteren Forschungen verdanken, wird nur in den Anmerkungen gelegentlich Erwähnung gethan werden.

Gauss hat im Laufe der Zeit acht Beweise für das quadratische Reciprocitätsgesetz geliefert. Von diesen veröffentlichte er selbst sechs, während die beiden anderen erst durch die Herausgabe seines Nachlasses bekannt geworden sind. Die Anordnung geschah im voraufgehenden Texte nach der Zeit ihrer Publication, wie dies auch in den gesammelten Werken geschehen ist. Die chronologische Reihenfolge der *Gauss*'schen Beweise ist eine andere. *L. Kronecker* hat hierüber einige Vermuthungen aufgestellt*), die aber von *Baumgart* (l. c. S. 101) mit grosser Wahrscheinlichkeit widerlegt worden sind. Nach *Baumgart* dürfte die zeitliche Anordnung die folgende sein:

I, II, VII, (VIII), III, IV, V, VI.

Bei der Wiedergabe der Beweise wurde von III, IV, V, VI eine genaue Uebersetzung geliefert; dies war durch die in sich abgeschlossene Form angängig, welche *Gauss* selbst seinen Beweisen ertheilt hat. Beim Beweise I wurden, um allzu bedeutendes Anschwellen des Umfanges zu vermeiden, kleinere, zumal historische Notizen unterdrückt. Beim Beweise II, der ganz in der Theorie der quadratischen Formen wurzelt, sind die entscheidenden Ueberlegungen in wörtlicher Uebertragung vorgelegt; in den Erläuterungen wurde durch eine kurze Uebersicht dem Leser eine Einführung gegeben, welche das Verständniss zu vermitteln wohl ausreichen wird.

Die Beweise VII und VIII (Werke II S. 233 und S. 234) konnten nicht aufgenommen werden, da bei ihrer Darstellung der fragmentarische Charakter der nachgelassenen Abhandlung zu stark überwog. Der Kern der Beweise liegt bei ihnen in der Vergleichung zweier Kriterien für die Lösbarkeit einer Congruenz zweiten Grades, welcher die beiden umfassendsten Kreistheilungsperioden genügen. Um dem Leser auch nach dieser Richtung Klarheit zu geben, ist in der letzten, dreizehnten Anmerkung der Beweis kurz entwickelt [[13]) S. 109].

Die beiden Bezeichnungen »Fundamentaltheorem« der höheren Arithmetik und »Reciprocitätsgesetz« für den in Rede stehenden Satz haben wir bereits angegeben. Die zweite Be-

*) Berichte. Berl. vom 22. April 1875. p. 272, Anm.

nennung stammt von *Legendre*, der sie schon im Jahre 1785 eingeführt hat; sie hat sich als die charakteristischere in der Litteratur erhalten. Die erste Benennung führt *Gauss* in den »Disquisitiones arithmeticae« ein und begründet ihre Wahl mit der Wichtigkeit des Satzes.

Im Paragraphen 151 der »Disquisitiones« schreibt sich *Gauss* die endgültige, einfache Formulirung des Reciprocitätsgesetzes zu (1801). *Legendre* erhebt in einem Briefe an *Jacobi* [Journ. f. M. 80, (1875) p. 217] hiergegen Einsprache und nimmt für sich die Priorität in Anspruch. *L. Kronecker**) hat festgestellt, dass *L. Euler* der Erste gewesen ist, der auf dem Wege der Induction das Gesetz erkannte und in übersichtlichen, der *Gauss*'schen Form ähnlichen Ausdruck brachte. *Gauss* selbst hatte in § 2 des Beweises III seine früheren Ansprüche zu Gunsten von *Legendre*'s Autorschaft zurückgezogen (1808).

Nach diesen allgemeineren Darlegungen gehen wir zu den Erläuterungen über, welche die einzelnen Beweise betreffen.

1) *Zu S. 3.* Die Voraussetzungen des ersten Beweises sind von elementarster Natur; sie verlassen nirgend das Gebiet der Congruenzen zweiten Grades.

Charakterisirt wird der erste *Gauss*'sche Beweis — der überhaupt der erste Beweis des Reciprocitätssatzes ist — von *L. Kronecker***) als »merkwürdige und scharfsinnige Deduction, welche ganz direct mit Ueberwindung aller Schwierigkeiten auf das Ziel losgehend fast wie eine Kraftprobe *Gauss*schen Genies erscheint«. *Dirichlet* sagt***), ihm sei der Beweis »immer merkwürdig erschienen, sowohl wegen des so einfachen Gedankens, welcher demselben zu Grunde liegt, als auch deshalb, weil dieser Beweis der einzige ist, in welchem die Betrachtung das Gebiet der Congruenzen zweiten Grades, welchem der Satz wesentlich angehört, nirgend verlässt«.

2) *Zu S. 21.* Dass für 19 und 23 wirklich $4a^2 < 2p$ ist, sieht man unmittelbar. Wenn ferner $p > 23$ ist, dann wird $\sqrt{p} - 2 > \sqrt{8}$, und daraus folgt durch Quadrirung

$$p - 4\sqrt{p} > 4 \text{ und } p > 4 + 4\sqrt{p}.$$

---

*) Berichte, Berl. v. 22. April 1875.
**) Berichte, Berl. v. 22. Juni 1870.
***) Journ. für Math. 47 (1854), p. 139.

Nun ist nach der Annahme $2a < \sqrt{p} + 2$ und also

$$4a^2 < p + (4\sqrt{p} + 4), \text{ also } < p + p = 2p.$$

3) *Zu S. 23.* Denn statt der Reihe

$$a, a + 1, a + 2, \ldots a + n - 1$$

betrachten wir zunächst die Reihe

$$a - r, a - r + 1, a - r + 2, \ldots a - r + n - 1.$$

Hierin kommen mindestens so viele durch h theilbare Glieder vor wie in der Reihe der Zahlen $1, 2, 3, \ldots n$. Das zeigt den Satz; denn jedem durch h theilbaren Gliede der Reihe $a - r, a - r + 1, \ldots$ entspricht eins in $a, a + 1, a + 2, \ldots$, welches $\equiv r \pmod{h}$ ist.

4) *Zu S. 24.* Wir setzen $a \equiv r^2 \bmod. 2^\nu m$, wobei m ungerade und $\nu \geqq 3$ ist. Dann wird, wenn wir $r_1 = 2^{\nu-1}m - r$ setzen, zugleich auch $a \equiv r_1^2 \bmod. 2^\nu m$. Nun ist

$$\frac{a - r^2}{2^\nu m} + \frac{a - r_1^2}{2^\nu m} = 2\frac{a - r^2}{2^\nu m} + r - 2^{\nu-2}m.$$

Dabei ist der Annahme nach $\frac{a - r^2}{2^\nu m}$ ganz, das erste Glied auf der rechten Seite der letzten Gleichung also gerade, und das letzte wegen $\nu > 2$ gleichfalls. Dagegen ist r ungerade, und daher auch die ganze Summe rechts. Folglich ist die Summe der beiden Brüche links eine ungerade Zahl und deshalb einer unter ihnen selbst gerade. Somit ist die eine der Differenzen $a - r^2$, $a - r_1^2$ durch $2^{\nu+1}m$ theilbar.

5) *Zu S. 27.* Das Fundamentaltheorem liefert nämlich unmittelbar:

Wenn	pRa	pNa	pRb	pNb,
dann ist	aRp	aNp	$-bRp$	$-bNp$.

Benutzt man nun die Resultate aus § 111 und § 98, so folgt:

Wenn	$\pm pRa$	$\begin{Bmatrix} +pNa \\ -pRa \end{Bmatrix}$	$\begin{Bmatrix} pRb \\ -pNb \end{Bmatrix}$	$\begin{Bmatrix} +pNb \\ -pNb \end{Bmatrix}$,
dann ist	aRp	aNp	$-bRp$	$-bNp$;

und setzt man endlich für p einmal a und einmal b ein, so entstehen die Formeln des Textes.

6) *Zu S. 37. Dirichlet* sagt l. c. über diesen Beweis: »Wenn er die Kürze vermissen lässt, welche einige der späteren in

so hohem Grade auszeichnet, so liegt dieser Mangel nicht im Wesen der Methode und hat vielmehr seinen Grund in dem zufälligen Umstande, dass zur Darstellung gewisser Beziehungen, welche bei dieser Behandlungsweise häufig wiederkehren, kein zur Rechnung geeignetes Zeichen benutzt ist, wodurch es nöthig geworden ist, acht verschiedene Fälle zu unterscheiden, von denen jeder wieder in mehrere Unterabtheilungen zerfällt. Durch Einführung des zuerst von *Legendre* gebrauchten Zeichens in der allgemeinen Bedeutung, welche *Jacobi* demselben später gegeben hat, und durch einige andere Vereinfachungen, welche jedoch das Wesen des Beweises eben so wenig ändern, zieht sich dieser in einem solchen Grade zusammen, dass er kaum noch hinter einem der übrigen hinsichtlich der Kürze zurückzustehen scheint.«

Was zunächst die erwähnte *Legendre*'sche Bezeichnung anlangt, so ist diese die folgende. *Legendre* setzt das Symbol, in welchem q eine Primzahl bedeutet,

$$\left(\frac{p}{q}\right) \text{ gleich } +1 \text{ oder gleich } -1$$

je nachdem in *Gauss*'scher Bezeichnung

$$pRq \quad \text{oder} \quad pNq$$

d. h. je nachdem p ein quadratischer Rest oder ein quadratischer Nichtrest für den Modul q wird; p soll dabei nicht durch q theilbar sein. Die Restcharaktere nehmen dann, wenn p und q ungerade Primzahlen sind, die Formen an

$$(\alpha)\quad \left(\frac{-1}{p}\right) = (-1)^{\frac{1}{2}(p-1)}; \qquad (\beta)\quad \left(\frac{2}{p}\right) = (-1)^{\frac{1}{8}(p^2-1)};$$

$$(\gamma)\quad \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{1}{2}(p-1)\frac{1}{2}(q-1)}.$$

Für das *Legendre*'sche Symbol ist, wenn p_1, p_2 zwei beliebige durch q nicht theilbare Zahlen bedeuten,

$$\left(\frac{p_1}{q}\right)\left(\frac{p_2}{q}\right) = \left(\frac{p_1 p_2}{q}\right).$$

Jacobi definirt nun*): Ist p irgend eine ungerade Zahl $= f \cdot f' \cdot f'' \ldots\ldots$ wo $f, f', f'' \ldots\ldots$ gleiche oder verschiedene

* Berichte. Berl. 1837. Octob. — Journ. f. M. 30 (1837), S. 166 — Werke VI S. 254—264 S. 262

Primzahlen bedeuten, so dehne ich die schöne *Legendre*'sche Bezeichnung auf zusammengesetzte Zahlen p in der Art aus, dass ich mit $\left(\frac{x}{p}\right)$, wenn x zu p Primzahl ist, das Product

$$\left(\frac{x}{p'}\right)\left(\frac{x}{p''}\right)\left(\frac{x}{p'''}\right)\cdots$$

bezeichne. Sind p und q zwei ungerade Zahlen, die keinen gemeinsamen Theiler haben, beide positiv oder auch die eine positiv, die andere negativ, so hat man ganz wie bei Primzahlen die obigen Gleichungen (α), (β), (γ).

Durch die Einführung und die Benutzung dieses *Jacobi*'schen Symbols vereinfacht sich der erste *Gauss*'sche Beweis. Es ist übrigens zu bemerken, dass *Gauss* selbst die Bedeutung dieses Symbols erkannt hat. Das in § 139 der Disquisitiones eingeführte Zeichen $[x, y]$ giebt die Anzahl der Primfactoren von y an, von denen x Nichtrest ist. Man hat demnach, wenn die rechte Seite der folgenden Congruenz das *Jacobi*'sche Symbol enthält,

$$[p, q] \equiv \left(\frac{p}{q}\right) \pmod{2}.$$

Für das Studium des *Dirichlet*'schen Beweises empfehlen wir nebst der Originalabhandlung die Darstellung, welche sich in der von *Dedekind* herausgegebenen Ausgabe der »Vorlesungen über Zahlentheorie von *P. G. Lejeune Dirichlet*« findet.

Wir wollen, um wenigstens eine der von *Dirichlet* gegebenen Vereinfachungen hier zu besprechen, den Hülfssatz aus § 129 der »Disquisitiones« in *Dirichlet*'scher Art beweisen. Es handelt sich darum, dass eine Zahl $p' < q$ existirt, für die q Nichtrest ist, wenn $q = 8n + 1$ angenommen wird.

Es sei $2m + 1 < q$, und man nehme an, q sei quadratischer Rest von allen ungeraden Primzahlen, welche nicht grösser als $2m + 1$ sind. [Wegen $q = 8n + 1$ ist q auch Rest der Potenzen von 2 und es ist] dann die Congruenz $x^2 \equiv q$ für jeden Modul lösbar, der ausser einer beliebigen Potenz von 2 nur ungerade, $2m + 1$ nicht übertreffende Primfactoren enthält. Diese Bedingungen erfüllt aber das Product $1 . 2 . 3 \ldots 2m + 1 = M$, und man kann also setzen $k^2 \equiv q \pmod{M}$, wo k positiv gewählt ist. Man hat dann

$$(q - 1^2)(q - 2^2) \ldots (q - m^2) \equiv (k^2 - 1^2)(k^2 - 2^2) \ldots$$
$$\ldots (k^2 - m^2) \pmod{M}.$$

Nun lässt sich die zweite Seite, wenn man sie mit dem Factor k multiplicirt, der relative Primzahl zu M ist, als continuirliches Product

$$(k+m)(k+m-1)\ldots(k-m)$$

schreiben, welches Product ein Vielfaches von M ist, wie sich leicht rein arithmetisch zeigen lässt, und wie dies auch daraus folgt, dass dasselbe, durch M dividirt, eine Combinationszahl darstellt. Es muss also auch die erste Seite durch M getheilt werden können. Giebt man dem Quotienten dieser Division die Form

$$\frac{1}{m+1}\cdot\frac{q-1^2}{(m+1)^2-1^2}\cdot\frac{q-2^2}{(m+1)^2-2^2}\cdots\frac{q-m^2}{(m+1)^2-m^2},$$

so stellt sich offenbar ein Widerspruch heraus, wenn man für m diejenige ganze Zahl wählt, welche unmittelbar unter $\sqrt{q}$ liegt, indem dann der Quotient ein Product echter Brüche wird. Es ist daher stillschweigend angenommen, dass diese Wahl der Zahl m der Bedingung $2m+1 < q$, die unserer Deduction zu Grunde liegt, gemäss ist, was wirklich der Fall ist, da $2m+1 < 2\sqrt{q}+1$ und $2\sqrt{q}+1$ augenscheinlich für alle Primzahlen $8n+1$, deren kleinste 17 ist, < 9 ist. Es ist somit bewiesen, dass es immer eine Primzahl p' giebt, welche $< 2m+1 < q$ ist und für welche q ein quadratischer Nichtrest ist.«

7) *Zu S. 10.* Wie wir schon erwähnt haben, ist dieser zweite Beweis derart in die Theorie der quadratischen Formen verflochten, dass es unmöglich erscheint, ihn so geschlossen und vollständig aus den allgemeineren Untersuchungen herauszuschälen, wie dies beim ersten Beweise möglich war; es sei denn, dass man geradezu die gesammten umfangreichen Ableitungen des fünften Abschnittes der »Disquisitiones« wiedergäbe.

Um aber trotzdem den Gedankengang dieses hocheleganten Beweises dem Verständniss zu erschliessen, sollen im Folgenden ohne Beweise und mit Einhaltung möglichster Kürze die Grundlagen, auf denen es beruht, vollständig gegeben werden. Die eingeschalteten Paragraphenzahlen beziehen sich auf die Stellen der »Disquisitiones«, denen die angeführten Sätze entnommen sind.

Jeder Ausdruck $ax^2+2bxy+cy^2=F$ wird als quadratische Form, oder, wenn kein Missverständniss eintreten

kann, wohl auch kurz als **Form** bezeichnet. Dabei sind a, b, c gegebene ganze Zahlen und x, y ganze unbestimmte Zahlen. Handelt es sich nicht um diese Unbestimmten x, y, dann wird $F = (a, b, c)$ geschrieben (§ 153). Wenn

$$M = am^2 + 2bmn + cn^2$$

ist, wobei m und n theilerfremd zu einander sind, dann sagt man, M werde durch (a, b, c) **dargestellt**. Der Ausdruck $b^2 - ac = D$ heisst die **Determinante** der Form F. D ist quadratischer Rest jeder durch (a, b, c) darstellbaren Zahl M (§ 154). Wird F bei ganzzahligen

$$\alpha, \beta, \gamma, \delta \text{ und } \alpha\delta - \beta\gamma = \pm 1$$

durch $x = \alpha x' + \beta y'$ und $y = \gamma x' + \delta y'$ in

$$F' = a'x'^2 + 2b'x'y' + c'y'^2 = (a', b', c')$$

transformirt, so wird umgekehrt F' durch $\pm x' = \delta x - \beta y$, $\pm y' = -\gamma x + \alpha y$ in F transformirt. Daher ist jede, durch eine der beiden Formen darstellbare Zahl auch durch die andere, transformirte darstellbar. Die Determinanten beider Formen sind einander gleich. Zwei solche, gegenseitig in einander transformirbare Formen heissen einander **äquivalent** und zwar sind sie **eigentlich** oder **uneigentlich äquivalent**, je nachdem $\alpha\delta - \beta\gamma = +1$ oder $= -1$ ist. Eine Form kann einer anderen gleichzeitig eigentlich und uneigentlich äquivalent sein (§ 157, 158, 163).

Alle Formen derselben Determinante D, welche einander eigentlich äquivalent sind, rechnen wir einer **Classe von Formen** zu (§ 175). Die **Anzahl der Classen** einer gegebenen Determinante ist endlich (§ 175, § 195, § 211). Besitzt die Form $F = (a, b, c)$ eine negative Determinante D, so haben die äusseren Coefficienten a und c gleiche Vorzeichen, und dieses Vorzeichen ist für alle Formen derselben Classe das gleiche. Ist es positiv (bezw. negativ), so heisst die Form selbst eine **positive** (bezw. eine **negative**); dementsprechend heissen dann auch die enthaltenden Classen **positive** und **negative Classen**. Durch eine positive Form lassen sich keine negativen, durch eine negative Form keine positiven Zahlen darstellen (§ 175, § 225).

Eine Form F heisst eine **primitive Form**, wenn a, b, c keinen gemeinsamen Theiler haben; anderenfalls heisst F eine **derivirte Form**. Kommt in einer Formenclasse eine primitive Form vor, so sind alle zugehörigen Formen primitiv, und

die Classe heisst eine **primitive Classe**. Haben auch a, $2b$, c keinen gemeinsamen Theiler, so heisst die Form **eigentlich primitiv**; alle Formen der zugehörigen Classe sind auch eigentlich primitiv, und die Classe heisst eine **eigentlich primitive Classe**. Besteht für a, b, c kein Theiler, dagegen für a, $2b$, c, dann heissen Form und Classe **uneigentlich primitiv** (§ 226).

Die beiden Classen, denen die Formen (a, b, c) bezw. (a', b', c') angehören, werden zu gleicher **Ordnung** gerechnet, wenn sowohl a, b, c denselben grössten gemeinsamen Theiler haben wie a', b', c', als auch $a, 2b, c$ denselben grössten gemeinsamen Theiler haben wie $a', 2b', c'$. Ist dies nicht der Fall, dann werden die Classen zu verschiedenen Ordnungen gerechnet. So bilden z. B. alle eigentlich primitiven Formenclassen eine Ordnung für sich; und eben das Gleiche gilt von allen uneigentlich primitiven Classen (§ 226).

Eine eigentlich primitive Ordnung kann wieder in **Geschlechter** eingetheilt werden. Das geschieht auf Grund folgender Sätze: Ist F eine zur Determinante D gehörige primitive Form, und p eine in D aufgehende Primzahl, dann sind alle durch p nicht theilbaren Zahlen, welche durch F dargestellt werden können, entweder sämmtlich quadratische Reste von p oder sämmtlich quadratische Nichtreste von p. — Wenn ferner D durch 4 theilbar ist, dann sind die durch F darstellbaren ungeraden Zahlen entweder sämmtlich $\equiv 1$ (mod. 4) oder sämmtlich $\equiv 3$ (mod. 4). Wenn D durch 8 theilbar ist, dann sind die durch F darstellbaren ungeraden Zahlen entweder sämmtlich $\equiv 1$ oder sämmtlich $\equiv 3$ oder $\equiv 5$ oder $\equiv 7$ (mod. 8); für $D \equiv 3$ (mod. 4) sind sie entweder sämmtlich $\equiv 1$ oder sämmtlich $\equiv 3$ (mod. 4); für $D \equiv 2$ (mod. 8) sind sie sämmtlich theils $\equiv 1$, theils $\equiv 7$, oder sämmtlich theils $\equiv 3$, theils $\equiv 5$ (mod. 8); für $D \equiv 6$ (mod. 8) sind sie sämmtlich theils $\equiv 1$, theils $\equiv 3$ oder sämmtlich theils $\equiv 5$, theils $\equiv 7$ (mod. 8). Jede solche Eigenschaft nennt *Gauss* einen **Charakter** der Form F und bezeichnet die einzelnen soeben angeführten Charaktere der Reihe nach durch

Rp oder Np; 1, 4 oder 3, 4; 1, 8 oder 3, 8 oder 5, 8 oder 7, 8; 3 *und* 5, 8 oder 1 *und* 7, 8; 1 *und* 3, 8 oder 5 *und* 7, 8. (§ 229, § 230).

Der **Totalcharakter** einer Form oder einer Classe setzt sich aus sämmtlichen einzelnen Charakteren der Form oder

der Classe zusammen. Die Ordnung der eigentlich primitiven (und wenn die Determinante negativ ist, zugleich: der positiven) Classen von gegebener Determinante wird derart in Geschlechter eingetheilt, dass zwei Classen zu demselben Geschlechte gerechnet werden, wenn sie denselben Totalcharakter besitzen (§ 231). Bei negativer Determinante heissen die Geschlechter, welche nur positive Classen enthalten, positive Geschlechter. — Die Form (1, 0, — D) der Determinante D heisst Hauptform; die Classe, der sie angehört, heisst Hauptclasse, und das Geschlecht, dem diese Classe angehört, heisst das Hauptgeschlecht (§ 231).

In den einzelnen Geschlechtern einer und derselben Ordnung einer gegebenen Determinante sind gleich viele Classen enthalten (§ 252).

Nicht mehr als der Hälfte aller, für eine gegebene, nicht quadratische Determinante als möglich angebbarer Totalcharaktere können eigentlich primitive (und bei negativer Determinante zugleich: positive) Geschlechter entsprechen (§ 261).

8) *Zu S. 10.* Bei den Determinanten — 1, + 2, — 2, — 4 kommen nämlich nur die beiden Charaktere hinsichtlich 4 und 8 in Frage. Bei den ungeraden Potenzen der Primzahl p von der Form $4n + 1$ giebt es nur die beiden Charactere für dieses p; die negativ genommenen Potenzen dieser Primzahlen sind sämmtlich $\equiv 3$ (mod. 4) und sind also, da bei ihnen dann vier Charaktere möglich wären, von der Betrachtung auszuschliessen. Aus dem gleichen Grunde kommen nur die positiv genommenen geraden und die negativ genommenen ungeraden Potenzen der Primzahlen von der Form $4n + 3$ in Frage; Quadrate sind ja ausgeschlossen.

Die im folgenden Absatze des Textes benutzten Charactere ergeben sich aus den zugehörigen Hauptformen (1, 0, — D).

9) *Zu S. 11.* *Kummer* sagt (l. c.): »Zwei [der späteren Beweise] nämlich der als dritter und fünfter von *Gauss* bezeichnete, sind beinahe ebenso elementar als der erste Beweis, da sie nur in so fern das Gebiet der Congruenzen zweiten Grades verlassen, als ein Satz über die reinen Congruenzen höherer Grade hinzugezogen wird.« — Der Unterschied dieser Beweise liegt hauptsächlich nur in der Art der Abzählung der Reste.«

Jener Satz über die reinen Congruenzen höherer Grade ist das in § 106 der »Disquisitiones« abgeleitete Kriterium.

10) *Zu S. 47.* Im Falle $p = 4n + 1$ ist das letzte umzuwandelnde Glied

$$\left[\frac{\frac{1}{2}(p+3)k}{p}\right] = k - 1 - \left[\frac{\frac{1}{2}(p-3)k}{p}\right],$$

und die obere Reihe jenes Ausdruckes in VI wird, da $\frac{p-1}{4}$ Summanden umgewandelt sind,

$$\tfrac{1}{4}(p-1)(k-1) + \left\{\left[\frac{2k}{p}\right] + \left[\frac{4k}{p}\right] + \cdots + \left[\frac{\frac{1}{2}(p-1)k}{p}\right]\right\}$$
$$- \left\{\left[\frac{k}{p}\right] + \left[\frac{3k}{p}\right] + \cdots + \left[\frac{\frac{1}{2}(p-3)k}{p}\right]\right\}.$$

Vereinigt man mit den Gliedern der ersten geschweiften Klammer die mit -2 multiplicirten gleichen Glieder der unteren Reihe, dann ergiebt sich das erste Resultat.

Im Falle $p = 4n + 3$ ist das letzte umzuwandelnde Glied

$$\left[\frac{\frac{1}{2}(p+1)k}{p}\right] = k - 1 - \left[\frac{\frac{1}{2}(p-1)k}{p}\right],$$

und die obere Reihe jenes Ausdruckes in VI wird, da jetzt $\frac{p+1}{4}$ Summanden umgewandelt sind,

$$\tfrac{1}{4}(p+1)(k-1) + \left\{\left[\frac{2k}{p}\right] + \left[\frac{4k}{p}\right] + \cdots + \left[\frac{\frac{1}{2}(p-3)k}{p}\right]\right\}$$
$$- \left\{\left[\frac{k}{p}\right] + \left[\frac{3k}{p}\right] + \cdots + \left[\frac{\frac{1}{2}(p-1)k}{p}\right]\right\}.$$

Daraus folgt dann in ähnlicher Art das zweite Resultat.

11) *Zu S. 51.* Der vierte und der sechste *Gauss*'sche Beweis stützen sich auf die Theorie der Kreistheilung, insbesondere auf die Ausnützung einer Formel, deren Ableitung hier nach *Gauss*, Disquisitiones § 356 gegeben werden soll.

Es sei $n = 2m + 1$ eine Primzahl, r eine primitive n^{te} Wurzel der Einheit und g eine primitive Congruenzwurzel für den Modul n, d. h. eine zum Exponenten $2m$ gehörige Zahl. Dann sind alle primitiven n^{ten} Wurzeln der Einheit in dem Complexe enthalten:

$$r^{g^0},\ r^{g^1},\ r^{g^2},\ r^{g^3},\ \ldots\ r^{g^{n-2}}$$

oder, wie wir bequemer schreiben wollen, in

$$[g^0],\ [g^1],\ [g^2],\ [g^3],\ \ldots\ [g^{n-2}].$$

Wir vertheilen diese Wurzeln in zwei **Perioden**

$$(m, g^0) = [g^0] + [g^2] + [g^4] + \cdots + [g^{n-3}],$$
$$(m, g^1) = [g^1] + [g^3] + [g^5] + \cdots + [g^{n-2}];$$

die Gleichung, deren Wurzeln diese beiden Aggregate sind, möge

$$x^2 - Ax + B = 0$$

sein, wobei also

$$A = (m, 1) + (m, g) = -1; \quad B = (m, 1) \cdot (m, g)$$

gesetzt ist. Bildet man B durch Ausmultipliciren, so folgt

$$B = (m, g^1 + 1) + (m, g^3 + 1) + (m, g^5 + 1) + \cdots$$
$$+ (m, g^{n-2} + 1).$$

Jeder Summand links ist entweder (m, g^0) oder (m, g^1) oder m und also

$$B = \alpha \cdot m + \beta \cdot (m, 1) + \gamma \cdot (m, g), \quad (\alpha + \beta + \gamma = m).$$

Ferner ergiebt die allgemeine Theorie, dass B eine ganze Zahl, folglich $\beta = \gamma$ und daher

$$B = \alpha \cdot m - \beta; \quad \alpha + 2\beta = m$$

ist.

Um α zu bestimmen, unterscheiden wir zwei Fälle:

1) Es sei m ungerade. Da $g^m + 1 \equiv 0$ (mod. n) ist, so giebt es in der Reihe

$$g + 1,\ g^3 + 1,\ g^5 + 1,\ \ldots\ g^{n-2} + 1$$

ein Glied und nur ein Glied $\equiv 0$ (mod. n); folglich ist $\alpha = 1$ und daher $\beta = \frac{1}{2}(m - 1)$. Dies ergiebt

$$B = \tfrac{1}{2}(m + 1).$$

2) Es sei m gerade. In diesem Falle giebt es in der Reihe

$$g + 1,\ g^3 + 1,\ g^5 + 1,\ \ldots\ g^{n-2} + 1$$

kein Glied, welches $\equiv 0$ (mod. n) wäre; folglich ist $\alpha = 0$ und daher $\beta = \frac{1}{2} m$. Dies ergiebt

$$B = -\tfrac{1}{2} m.$$

Die Gleichung für x ist in diesen beiden Fällen

$$x^2 + x + \tfrac{1}{2} m + 1 = 0, \text{ wenn } n \text{ die Form } 4k + 3 \text{ hat},$$
$$x^2 + x - \tfrac{1}{2} m \qquad = 0, \text{ wenn } n \text{ die Form } 4k + 1 \text{ hat},$$

oder allgemein

$$x^2 + x + \tfrac{1}{4}\left(1 - (-1)^{\frac{n-1}{2}} n\right);$$

und folglich ist

$$x = -\tfrac{1}{2} \pm \tfrac{1}{2} i \sqrt{n}, \text{ wenn } n \text{ die Form } 4k + 3 \text{ hat},$$
$$x = -\tfrac{1}{2} \pm \tfrac{1}{2} \sqrt{n}, \text{ wenn } n \text{ die Form } 4k + 1 \text{ hat},$$

oder allgemein

$$x = -\tfrac{1}{2} \pm \tfrac{1}{2}\sqrt{(-1)^{\frac{n-1}{2}} n}.$$

Daher wird auch

$$[m, g^0] - [m, g^1] = \pm \sqrt{n}, \text{ wenn } n \text{ die Form } 4k + 1 \text{ hat},$$
$$[m, g^0] - [m, g^1] = \pm i \sqrt{n}, \text{ wenn } n \text{ die Form } 4k + 3 \text{ hat};$$

und zwar gilt dies, welche Wurzel auch für $[g^0] = r$ genommen werden mag.

Ferner ist

$$[g^a] = r^{g^a} = \left(\cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n}\right)^{g^a}$$
$$= \cos\frac{1}{n} 2\pi g^a + i \sin\frac{1}{n} 2\pi g^a.$$

In $[m, g^0]$ durchlaufen die g^a alle quadratischen Reste von n, in $[m, g^1]$ dagegen alle quadratischen Nichtreste. Diese Bemerkung liefert dann die in § 1 des vierten Beweises angeführten Formeln.

Der vierte Beweis benutzt die Bestimmung des bis jetzt noch zweifelhaften Vorzeichens von $[m, g^0] - [m, g^1]$; der sechste Beweis kommt ohne diese Bestimmung zum Ziele.

Speciell über den vierten Beweis spricht sich *L. Kronecker** folgendermaassen aus: »Die gesammte Schwierigkeit lag in der Summirung von

$$\sum_{h=0}^{p-1} \cos\frac{2h^2\pi}{p} \quad \text{und} \quad \sum_{h=0}^{p-1} \sin\frac{2h^2\pi}{p} \quad (p \text{ Primzahl}).$$

* Vorlesungen aus der Theorie der einfachen und der vielfachen Integrale. Leipzig, Teubner. 1894. p. 117, 118.

aus welcher dann das quadratische Reciprocitätsgesetz leicht zu entnehmen war. *Gauss* hat wahrscheinlich schon in seinem siebzehnten Jahre den Werth der Reihen, abgesehen vom Vorzeichen, gefunden, dessen Bestimmung ihm, wie aus der Abhandlung »Summatio quarundam serierum singularium« und aus einem Briefe an *Sophie Germain* hervorgeht, unsägliche Mühe machte. Nach sechsjähriger andauernder Beschäftigung mit dem Gegenstande glückte ihm die Feststellung des Zeichens und zwar, wie er in bewundernswerther Bescheidenheit sagt, nur durch eine Art Eingebung. Ueber seinen Gedankengang hat er uns völlig im Dunkel gelassen, und in der That ist seine Beweisart auch noch heute ein Räthsel. Er hat gleichsam aus einer Projection die ganze Figur erhalten, indem er nämlich aus einer specielleren eine allgemeinere Reihe errieth und diese dann als ein Sinus-Product darstellte. Bisher ist es übrigens noch nicht gelungen, eine Summe von Sinus, wie sie in der Reihe vorliegt, direct in ein solches Product umzuformen. Ausserdem ist es merkwürdig, dass *Gauss*, obwohl er nahe daran war, doch nicht darauf gekommen ist, die ihm bekannte Θ-Reihe zur Berechnung seiner Summe zu benutzen.«

12) *Zu S.* 88. *E. Kummer* sagt l. c. über diesen sechsten Beweis: »Der eigentliche Kern dieses Beweises wird bei *Gauss* dadurch etwas verhüllt, dass anstatt der p^{ten} Wurzel der Einheit eine unbestimmte Variabele x angewendet wird, was zur Folge hat, dass Congruenzen unter ganzen rationalen Functionen nach dem Modul $1+x+x^2+\cdots+x^{p-1}$ angewendet werden müssen, statt deren man nur einfache Gleichungen erhält, wenn dem x der specielle Werth einer primitiven p^{ten} Wurzel der Einheit gegeben wird. Diese Vereinfachung des sechsten *Gauss*'schen Beweises hat zuerst *Jacobi* ausgeführt und im Jahre 1827 an *Legendre* mitgetheilt, welcher sie im Jahre 1830 in die dritte Ausgabe seiner »Théorie des nombres« aufgenommen hat. *Eisenstein* hat denselben Beweis im Jahre 1844 in *Crelle*'s Journal Band 28, S. 41 reproducirt.«

Um die Vereinfachungen zu zeigen, welche durch diese *Jacobi*'sche Annahme hervorgerufen werden, wollen wir den Beweis nach *Legendre* (Théorie des nombres: édit. 3. Bd. II S. 391) reproduciren.

Es sei $p = 2m + 1$ irgend welche ungerade Primzahl, g eine der zu ihr gehörigen primitiven Congruenzwurzeln, so

dass $g^m + 1 \equiv 0 \mod. p$ ist. Dann können alle Wurzeln von $X = \frac{x^p - 1}{x - 1} = 0$ durch die Glieder der Reihe

$$[1], \ [g], \ [g^2], \ [g^3], \ldots [g^{2m-1}]$$

dargestellt werden. Setzen wir

$$y_0 = [1] + [g^2] + [g^4] + \cdots + [g^{2m-2}],$$
$$y_1 = [g] + [g^3] + [g^5] + \cdots + [g^{2m-1}],$$

so ist (vgl. Anm. 11)

$$y_0 = -\tfrac{1}{2} \pm \tfrac{1}{2} \sqrt{(-1)^{\frac{p-1}{2}} p}, \quad y_1 = -\tfrac{1}{2} \mp \tfrac{1}{2} \sqrt{(-1)^{\frac{p-1}{2}} p}.$$

Wir bezeichnen

$$P = [1] - [g] + [g^2] - [g^3] + \cdots + [g^{2m-2}] - [g^{2m-1}]$$

und haben

$$P = \pm \sqrt{(-1)^{\frac{p-1}{2}} p}.$$

Nun sei q irgend eine von p verschiedene Primzahl; wir wollen P in die q^{te} Potenz erheben. Diese Potenz enthält zuerst die q^{ten} Potenzen der verschiedenen Glieder des Polynoms P, jedes einzeln potenzirt; und da

$$[g^\alpha]^q = [g^\alpha q] = [qg^\alpha]$$

ist, so besteht dieser erste Theil aus den Gliedern

$$Q = [q] - [qg^1] + [qg^2] - \cdots + [qg^{2m-2}] - [qg^{2m-1}].$$

Ausserdem enthält P^q nur noch Glieder von der Form qAx^α. Wir können demnach schreiben

$$P^q = Q + \sum qAx^\alpha.$$

Welchen Werth die von p verschiedene Primzahl q auch immer haben möge, stets ist entweder $\left(\frac{q}{p}\right) = 1$ oder $\left(\frac{q}{p}\right) = -1$. Im ersten Falle kann man $q \equiv g^{2r} \mod. p$ setzen; im zweiten Falle $q \equiv g^{2r+1} \mod. p$. Im ersten Falle wird dann

$$Q = [g^{2r}] - [g^{2r+2}] + \cdots + [g^0] - [g^1] + \cdots = P,$$

dagegen im zweiten Falle

$$Q = [g^{2r+1}] - [g^{2r+2}] + \cdots - [g^0] + [g^1] - \cdots = -P.$$

und also in beiden Fällen

$$R = \left(\frac{q}{p}\right) P$$

und

$$P^q = \left(\frac{q}{p}\right) P + q \sum A \varepsilon^{\alpha},$$

$$P^{q-1} - \left(\frac{q}{p}\right) = q \cdot \frac{\sum A \varepsilon^{\alpha}}{P}.$$

Trägt man links den oben angegebenen Werth von P ein, dann entsteht

$$p^{\frac{q-1}{2}} \cdot (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} - \left(\frac{q}{p}\right) = q \frac{\sum A \varepsilon^{\alpha}}{P}.$$

Da die linke Seite eine ganze Zahl ist, so gilt das Gleiche von der rechten Seite, und da $P = \pm \left(p \cdot (-1)^{\frac{p-1}{2}}\right)^{\frac{1}{2}}$ zu q theilerfremd ist, so geht P in $\sum A \varepsilon^{\alpha}$ auf, und wir können setzen

$$p^{\frac{q-1}{2}} \cdot (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} - \left(\frac{q}{p}\right) = q \cdot A_0,$$

wobei A_0 eine ganze Zahl bedeutet. Da ferner

$$p^{\frac{q-1}{2}} \equiv \left(\frac{p}{q}\right) \pmod{q}$$

ist, so folgt aus der letzten Gleichung

$$\left(\frac{p}{q}\right) \cdot (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} - \left(\frac{q}{p}\right) \equiv 0 \pmod{q}$$

und daraus die gesuchte Beziehung

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

13) *Zu S. 95.* Das Princip des siebenten und des achten *Gauss*'schen Beweises hat *Lebesgue* (Par. Comp. Rend. 51 (1860) p. 9) selbständig entdeckt und veröffentlicht, ehe der *Gauss*sche Nachlass herausgegeben war. Wir können auf Grund dieses Princips den Beweis folgendermaassen führen.

Setzen wir, wenn p eine ungerade Primzahl bedeutet, wie oben,

$$y_1 = [g^1] + [g^3] + [g^5] + \cdots + [g^{p-2}],$$
$$y_2 = [g^2] + [g^4] + [g^6] + \cdots + [g^{p-1}]$$

und allgemein

$$y_\alpha = [g^\alpha] + [g^{\alpha+2}] + [g^{\alpha+4}] + \cdots + [g^{p+\alpha-3}],$$

so wird für die ungerade Primzahl q

$$y_\alpha{}^q \equiv [qg^\alpha] + [qg^{\alpha+2}] + [qg^{\alpha+4}] + \cdots + [qg^{p+\alpha-3}] \pmod{q},$$

da die übrigen Glieder durch q theilbare Coefficienten haben. Setzt man

$$(\alpha) \quad q \equiv g^k \pmod{p},$$

so wird

$$y_\alpha{}^q \equiv [g^{\alpha+k}] + [g^{\alpha+k+2}] + \cdots \equiv y_{\alpha+k}.$$

Wir fragen nun, unter welchen Bedingungen die Congruenz

$$(\beta) \quad (y-y_1)(y-y_2) \equiv y^2 + y + \tfrac{1}{4}\left(1-(-1)^{\frac{p-1}{2}}\right) \equiv 0 \pmod{q}$$

Wurzeln besitzt. Es ist klar, dass dies stattfindet oder nicht, je nachdem

$$y_1 y_2 \cdot (1-y_1)(1-y_2) \cdot (2-y_1)(2-y_2) \cdots$$
$$\cdots (q-1-y_1)(q-1-y_2)$$

den Werth Null oder einen anderen Werth besitzt. Nun ist

$$y_\varkappa(y_\varkappa-1)(y_\varkappa-2)\cdots(y_\varkappa-q+1) \equiv y_\varkappa{}^q - y_\varkappa \pmod{q};$$

somit formt sich die Bedingung in die andere um, ob

$$(y_1{}^q - y_1)(y_2{}^q - y_2) \equiv (y_{\varkappa+1} - y_1)(y_{\varkappa+2} - y_2)$$

Null oder von Null verschieden ist. Das Erste oder das Zweite findet statt, je nachdem $k \equiv 0$ oder $k \equiv 1 \pmod{2}$ wird. Nach (α) heisst dies, dass (β) Lösungen hat oder nicht, je nachdem qRp oder qNp ist, d. h. in *Legendre*'schen Zeichen, je nachdem

$$(\gamma) \quad \left(\frac{q}{p}\right) = +1 \quad \text{oder} \quad \left(\frac{q}{p}\right) = -1$$

wird.

Setzt man andererseits in (β) ein $y = \frac{1}{2}(x-1)$, so entsteht

$$(\beta_1) \quad x^2 \equiv (-1)^{\frac{p-1}{2}} p \pmod{q}.$$

und dies zeigt, dass (β_1) oder (β) Lösungen hat, je nachdem

$$(\gamma_1) \quad \left(\frac{(-1)^{\frac{p-1}{2}}p}{q}\right) = +1 \quad \text{oder} \quad \left(\frac{(-1)^{\frac{p-1}{2}}p}{q}\right) = -1$$

ist. Die linke Seite geht nach S. 5, § 98 in

$$\left(\frac{(-1)^{\frac{p-1}{2}}}{q}\right)\left(\frac{p}{q}\right)$$

und dies nach S. 11, § 106 in

$$(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right)$$

über. Vergleicht man also hiernach (γ) und (γ_1), so folgt

$$(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = 1;$$

und das ist das Fundamentaltheorem für zwei ungerade Primzahlen.

Druck von Breitkopf & Härtel in Leipzig.

